UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN GÉNIE INDUSTRIEL

PAR
SIMON THERRIEN

DÉVELOPPEMENT D'UNE MÉTHODOLOGIE POUR DÉTERMINER LES OBJECTIFS DE FIABILITÉ DES SYSTÈMES IMPORTANTS POUR LA SÛRETÉ D'UNE CENTRALE NUCLÉAIRE DE TYPE CANDU

AVRIL 2006

SOMMAIRE

La Commission Canadienne de Sûreté Nucléaire (CCSN) exige la mise en œuvre de la norme S-98 « Programme de fiabilité des centrales nucléaires ». Cette démarche est entreprise dans un effort d'amélioration continue. Elle permet de garantir que la fiabilité des Systèmes Importants pour la Sûreté (SIS) des centrales nucléaires exploitées au Canada est assurée de façon structurée pour l'ensemble de l'industrie. Une des exigences de cette norme est d'identifier les SIS et d'établir leurs objectifs de fiabilité.

Une revue exhaustive de la littérature a permis de démontrer qu'il n'existait pas de méthodologie permettant de déterminer les objectifs de fiabilité des SIS. Le but de ce projet était donc d'en développer une applicable aux centrales nucléaires de type CANDU 600 et particulièrement pour celles qui n'utilisent pas encore l'Étude Probabiliste de Sûreté (ÉPS).

Une méthodologie a donc été développée. Elle est composée des 9 étapes suivantes :

1. Définir le concept d'objectif de fiabilité.
2. Recueillir les informations pertinentes concernant les SIS.
3. Évaluer la sévérité de la perte des fonctions de sûreté des SIS.
4. Déterminer une valeur préliminaire de l'objectif de fiabilité.
5. Évaluer la fréquence d'occurrence des défaillances majeures de procédé.
6. Développer des séquences d'événement et les évaluer par rapport aux objectifs de sûreté
7. Évaluer les arbres de défaillance des SIS de mitigation.
8. Compléter l'AMDEC des SIS, présenter leur criticité sur la matrice de risque et valider la cohérence des valeurs préliminaires.
9. Comparer avec les valeurs des autres centrales nucléaires canadiennes.

Cette méthodologie a été validée en l'appliquant à un groupe de SIS identifiés à la seule centrale nucléaire exploitée par Hydro-Québec. Voici les principaux résultats :

1. La fréquence totale d'occurrence des défaillances majeures de procédé calculée à l'aide des valeurs préliminaires des SIS de procédé est de 0,011 par an ce qui respecte le critère de défaillance « Simple» de 0,3 par an.
2. Les fréquences totales de fonte du cœur et de relâche importante de matières radioactives calculées à l'aide des séquences d'événement développées sont respectivement de 5,76E-06 et 2,45E-07 par an. Elles respectent les objectifs de sûreté qui sont de 10E-04 et 10E-05 par an.
3. La matrice de risque a permis de démontrer que les systèmes présentent un risque acceptable défini par le seul système spécial de sûreté (SSS) du groupe soit le système de refroidissement d'urgence du cœur (RUC)..
4. Finalement, les valeurs ont été comparées avec celles d'autres centrales et sont cohérentes.

Voici les objectifs de fiabilité obtenus pour chacun des SIS du groupe sélectionné :

SIS	État de fonctionnement	Objectif de fiabilité
RUC*	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-02
	PERCA +SDE 24 heures après	1E-02
SEU*	Centrale en puissance	1E-02
	Centrale à l'arrêt planifié	1E-02
	PERCA +SDE 24 heures après	1E-02
ESR*	Centrale en puissance	1E-04
	Centrale à l'arrêt planifié	1E-04
	Situation d'urgence	1E-04
Grosse PERCA**	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-03
	Situation d'urgence	1E-03
Modérateur*	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-03
	Situation d'urgence	1E-03

* Unités : année/année, **Unités : événement /année

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui ont contribué de près ou de loin à la réalisation de mon projet de maîtrise par leur support ou leur collaboration. Je tiens particulièrement à remercier M. Georges Abdul-Nour ing. Ph.D., directeur du projet et professeur à l'Université du Québec à Trois-Rivières ainsi que M. Dragan Komljenovic ing. Ph. D., co-directeur et ingénieur à la centrale nucléaire Gentilly-2 pour avoir contribué de manière significative à l'élaboration de ce document. Je tiens spécialement à remercier M. Raynald Vaillancourt, M. Daniel Boulay et M. Jacques Raza, ingénieurs à la centrale nucléaire Gentilly-2. La participation de ces personnes a permis d'ajouter une valeur inestimable au projet. De plus, je tiens à remercier M. Guy Hotte, chef de l'unité « Analyse et Fiabilité » ainsi que tous les membres de l'équipe Fiabilité pour leur aide précieuse. Je remercie aussi la « Direction de la Production Thermique et Nucléaire d'Hydro-Québec » pour m'avoir accordé l'opportunité de réaliser ce projet et les ressources nécessaires pour le mener à terme. Finalement, je remercie spécialement toute ma famille ainsi que ma copine, Valérie Gauthier, qui m'ont grandement supporté tout au long de ce projet.

AVERTISSEMENTS

Hydro-Québec se dégage de toute responsabilité quant à l'utilisation ou l'interprétation qui pourrait être faite des informations contenues dans ce rapport par une tierce partie. En aucun cas, Hydro-Québec ne saurait être tenue responsable de tout dommage ou préjudice quelconque lié à une utilisation ou une interprétation fautive de tout ce rapport ou d'une partie de ce rapport.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS ET DES ACRONYMES

AEC :	Atomic Energy Commission
AEU :	Alimentation Électrique d'Urgence
AIEA :	Agence Internationale de l'Énergie Atomique
ALARA :	As Low As Reasonably Achievable
AMDEC :	Analyse des Modes de Défaillance, de leurs Effets et leur Criticité
AR :	Centrale en ARrêt planifié
BCP :	Baisse Contrôlée de Puissance
BP :	Basse Pression
B/R :	Bâtiment Réacteur
Calo :	système Caloporteur
CANDU :	CANadian Deuterium Uranium
Cat.1 :	Alimentation électrique de Catégorie 1
Cat.2 :	Alimentation électrique de Catégorie 2
Cat.3 :	Alimentation électrique de Catégorie 3
Cat.4 :	Alimentation électrique de Catégorie 4
CCSN :	Commission Canadienne de Sûreté Nucléaire
COG :	CANDU Owners Group
DAP :	programme de Déclenchement Automatique des Pompes du caloporteur
DBE :	"Design Basis Earthquake"
EACL :	Énergie Atomique Canada Limitée
EAG :	État d'Arrêt Garanti
EBR :	Eau Brute de Refroidissement
ÉMS :	Étude Matricielle de Sûreté
EN :	Exploitation Normale
ÉPS :	Étude Probabiliste de Sûreté
ESR :	Système d'Eau de Service Re-circulée
ÉF :	Étude de Fiabilité
FS :	Fonction de Sûreté
GV :	Générateur de Vapeur
HP :	Haute Pression

ICRP :	International Commission on Radiological Protection
MIT:	"Massachusetts Institute of Technology"
MP:	Moyenne Pression
NRC :	Nuclear Regulatory Commission
PÉF :	Probabilité de se situer dans un État de Fonctionnement donné.
PEI:	Procédure d'Exploitation sur Incident
PERCA:	PERte de CAloporteur
P.P. :	Pleine Puissance
RCA :	Rapport de Condition Anormale
RSS :	"Reactor Safety Study"
RTA :	système de Refroidissement en Temps d'Arrêt
RUC :	Système de Refroidissement d'Urgence du Cœur
SAU#1 :	Système d'Arrêt d'Urgence #1
SAU#2 :	Système d'Arrêt d'Urgence #2
SCU :	Salle de Commande d'Urgence
SDE :	"Site Design Earthquake"
SEU :	Système d'Eau d'Urgence
SÉV :	SÉVérité
SF :	Source Froide
SIS :	Système Important pour la Sûreté
SRR :	Système de Régulation du Réacteur
SRS :	Système Relié à la Sûreté
SSS :	Système Spécial de Sûreté
UO_2 :	Uranium naturel
UR :	Situation d'URgence suite à un incident
VP :	Valeur Préliminaire
WANO :	"World Association Nuclear Operators"

GLOSSAIRE

Action de repli :	Action visant à se positionner dans un état de repli [1].
Arrêt :	État de centrale caractérisé par l'état d'arrêt garanti du réacteur. L'activation automatique des systèmes de sûreté peut être bloquée et les systèmes de support peuvent être en configuration anormale [15].
CANDU :	Réacteur nucléaire dans lequel le combustible est l'uranium naturel (sous forme de boulettes de dioxyde d'uranium) et qui utilise l'eau lourde comme modérateur et comme réfrigérant [36].
Centrale nucléaire :	Installation de réacteur à fission dont la fonction est de produire de l'électricité à une échelle commerciale [16].
Créditer :	Reconnaître que quelque chose est responsable d'un certain effet [17].
Danger :	Menace contre la sécurité ou la vie d'une personne ou d'une chose [36].
Défaillance :	Cessation de l'aptitude d'un élément à accomplir une fonction requise [36].

[1] Les définitions sans référence ont été adaptées dans le cadre des travaux ou encore sont tirées de documents internes d'Hydro-Québec

Défaillance de cause commune : Défaillance de plusieurs dispositifs ou composants qui sont dans l'incapacité de remplir leurs fonctions du fait d'un événement ou d'une cause spécifique unique [36].

Défaillance majeure de procédé : Défaillance d'un système relié à la sûreté qui, en l'absence de tous les systèmes spéciaux de sûreté, entraînerait une défaillance systématique du combustible ou un rejet important de matières radioactives hors de la centrale nucléaire. Une défaillance systématique est une défaillance du combustible à la suite d'un événement sans que le combustible ait présenté de défaut préalablement [17].

Défaut : Modification accidentelle affectant le fonctionnement normal [36].

Défense en profondeur : Principe à la base de la conception des installations nucléaires qui consiste en l'interposition de plusieurs niveaux de protection contre le relâchement de substances radioactives [2].

Délai de repli : Délai prescrit pour l'amorçage d'une action de repli lors d'un défaut. Ce délai vise à permettre la réparation et la requalification de l'équipement touché.

Disponibilité : Probabilité qu'un dispositif soit en état de remplir une fonction requise, à un instant donné et dans des conditions données [36].

État de repli : État sûr où doit être placé la centrale lors de certaines défaillances ou indisponibilité d'équipements. Ces états sont dépendants du type de défaillance ou d'indisponibilité et visent à minimiser l'impact de celles-ci.

Étude probabiliste de sûreté : Analyse complète et intégrée de la sûreté d'une centrale nucléaire ou d'un réacteur. L'étude tient compte de la probabilité et des conséquences de la défaillance des équipements ou des conditions transitoires, analyse sa probabilité, ses conséquences et la progression de l'incident. L'analyse fournit des données numériques qui donnent une mesure cohérente de la sûreté de la centrale ou du réacteur [15].

Événement initiateur : Consiste en une défaillance d'un système de procédé qui peut entraîner une perte de la capacité de refroidissement du combustible ou une augmentation de la puissance du réacteur au-delà de la capacité de refroidissement.

Exploitation normale : Tout état planifié d'une centrale nucléaire consécutif à des procédures normales d'exploitation préalablement approuvées. Cela comprend tout arrêt, toute exploitation en puissance (démarrage, variation en puissance, état stationnaire, mode

d'ajustement de la réactivité et suivi de charge) et les états initial, intermédiaire et fin de vie au cours desquels il peut y avoir rechargement du combustible, étalonnage, mise à l'essai, entretien et inspection.

Fiabilité : Probabilité pour un système d'accomplir correctement la fonction demandée pendant une période de temps spécifiée et dans des conditions de fonctionnement déterminées. [36].

Fonction de sûreté : Exigence de sûreté que doit assurer un système (ou un groupe de systèmes) lors d'un accident visant à limiter l'irradiation de la population et du personnel affecté au site. Ces fonctions satisfont aux exigences générales de sûreté suivantes :

- Procéder à l'arrêt du réacteur et le maintenir à l'état d'arrêt sûr pendant et après des états de fonctionnement et des situations accidentelles.
- Évacuer la chaleur résiduelle du cœur suite à un arrêt du réacteur pendant et après des états de fonctionnement et des situations accidentelles.
- Atténuer les rejets radioactifs et assurer que ces rejets se situent dans les limites prescrites pendant et après des états de fonctionnement et des situations accidentelles.

Grosse PERCA : Correspond à un débit de fuite qui dépasse celui d'une petite perte de fluide caloporteur primaire et qui pourrait résulter d'une rupture guillotine double ou

d'une rupture longitudinale du plus gros tuyau ou collecteur [17].

Limites prescrites : Limites à respecter découlant d'engagements réglementaires, d'études techniques ou autres analyses.

Marge de sûreté : Différence entre la valeur critique attribuée à un paramètre associé à la défaillance d'un système, d'un composant ou d'un phénomène et la valeur actuelle du paramètre. Elle permet de répondre aux incertitudes présentes dans la modélisation, les données et les analyses.

Mode de défaillance : Effet par lequel une défaillance est observée [36].

Partie intéressée : Groupe ou particulier qui a un intérêt plus ou moins direct dans la vie d'une entreprise et qui est susceptible d'être touché par une décision de l'entreprise. Il y a trois grandes catégories de parties prenantes : celles qui participent directement à la vie économique de l'entreprise (salariés, directions, actionnaires, conseils d'administration, fournisseurs, clients), celles qui observent ses modes de gestion (institutions, médias) et celles qui sont influencées par son activité (population, villes, régions, etc.). [36].

Petite PERCA : Correspond à un débit de fuite qui dépasse celui d'une très petite fuite de fluide caloporteur primaire et qui pourrait résulter d'une rupture guillotine double de

	la plus grosse conduite d'alimentation de canal de combustible [17]. Une très petite PERCA correspond à un débit de fuite pouvant atteindre le débit maximal d'une seule pompe d'appoint du circuit primaire [17].
Relâche importante:	Est considérée importante si plus de 1% du Cs-137 est relâché à l'environnement.
Risque :	Possibilité de blessure ou de perte définie par une mesure de la probabilité et de la gravité d'un effet néfaste sur la santé, les biens matériels, l'environnement et autres valeurs [5].
Risque résiduel :	Risque qui demeure après l'application de la totalité des stratégies de maîtrise des risques [5].
Source froide :	Doit être en mesure d'évacuer la totalité de la chaleur produite par le combustible sans que les températures atteintes présentent une menace pour l'intégrité du combustible et des tubes de force.
Système :	Ensemble fonctionnel dont les parties sont interconnectées et échangent de la matière, de l'énergie ou de l'information [36].
Système de mitigation :	Système susceptible d'éliminer ou de réduire les impacts négatifs d'un incident.
Système de procédé :	Système qui réalise la régulation et le refroidissement du cœur dans des conditions normales d'exploitation.

Système de sûreté en attente : Système qui doit permettre en tout temps la poursuite de la supervision des paramètres critiques, d'assurer l'arrêt du réacteur, le refroidissement du cœur et le confinement lors de conditions ultimes en centrale.

Système important pour la sûreté : Système relié à la sûreté associé à l'initiation, à la prévention, à la détection ou à l'atténuation de toute séquence de défaillance pouvant mener à l'endommagement du combustible ou au rejet associé de radio-nucléides et ***qui contribue de manière considérable à la sûreté*** de la centrale nucléaire.

Système relié à la sûreté : Système, structure, composant ou procédure (interventions de l'opérateur) et systèmes de soutien (y compris les systèmes spéciaux de sûreté et leurs systèmes de soutien) associés au déclenchement, à la détection ou à l'atténuation d'une séquence de défaillances pouvant entraîner un événement grave [17].

Système spécial de sûreté : Système conçu pour prévenir ou atténuer les conséquences d'une défaillance fonctionnelle et pour limiter les rejets de matières radioactives aux limites réglementaires.

CHAPITRE 1

INTRODUCTION

1.1 Mise en contexte

Les pays industrialisés consomment de grandes quantités d'énergie tandis que l'émergence de nouvelles puissances comme la Chine et l'Inde provoque une demande énergétique accrue qui entraîne un déséquilibre entre l'offre et la demande. En fait, les besoins énergétiques mondiaux sont sans cesse grandissants [39]. Ce phénomène se reflète par l'augmentation substantielle des prix dans le secteur de l'énergie. Dans ce contexte, la production mondiale d'énergie doit être augmentée de façon significative afin de combler la demande croissante. L'accroissement de la capacité de production ne doit pas se faire au détriment de l'environnement ou encore des générations futures et il doit tenir compte de plusieurs autres facteurs comme le vieillissement de la population, le coût élevé des nouvelles installations, leur durée de vie, etc. Des sources d'énergie compétitives respectant ces critères doivent donc être développées.

En matière de consommation d'énergie, le Québec ne fait pas exception. Même si la société québécoise peut se compter chanceuse d'avoir l'hydroélectricité, elle doit tout de même diversifier sa production dans le but de minimiser le risque de faire face à un déficit énergétique. Notre société est consciente du problème mais elle n'est pas prête à le régler à n'importe quel prix. Le rejet massif du projet du Suroît démontre bien que la production d'énergie contribuant à l'augmentation des gaz à effet de serre n'est pas acceptable.

Il existe une compétition féroce entre les diverses sources de production d'électricité comme les centrales hydrauliques, les centrales au charbon, les centrales au gaz, les centrales nucléaires, les éoliennes, l'énergie solaire, etc. [39]. Chacune d'entre elles

présente des avantages et des inconvénients. En fait, leurs bénéfices pour la société doivent dépasser leurs inconvénients avec une certaine marge acceptable pour la population.

Dans la mesure où elles sont économiquement compétitives, les centrales nucléaires pourraient constituer une solution temporaire à la crise énergétique mondiale en attendant que des sources d'énergie renouvelables soient développées. À l'heure actuelle, il n'existe pas encore d'alternative qui puisse à la fois remplacer les centrales utilisant les combustibles fossiles et celles de type nucléaire [37]. L'accord de Kyoto sur la réduction des gaz à effet de serre vient ajouter un argument favorable à l'utilisation de cette source d'énergie par rapport aux centrales au charbon ou au gaz. Cependant, l'avenir de l'industrie nucléaire fait face à une réévaluation en Amérique du Nord [2]. Le Canada est un bel exemple puisqu'une décision doit être prise quant à la réfection de la majorité des CANDU qui y sont en exploitation. À l'heure actuelle, la puissance nucléaire installée dans le monde assure environ 17% de la production mondiale d'électricité. Cependant, l'industrie nucléaire stagne puisque cette puissance installée correspond à celle du début des années 1990 [2]. Si l'industrie nucléaire veut assurer sa survie et accroître sa part de marché, elle doit absolument travailler à améliorer 4 aspects majeurs [6] :

1. Diminuer ses coûts de production et améliorer sa rentabilité;
2. Maintenir la sûreté de ses installations;
3. Élaborer une solution acceptable de gestion à long terme du combustible irradié et;
4. Présenter un risque négligeable de prolifération.

Les centrales nucléaires sont exploitées de façon à présenter un risque jugé acceptable pour la population. Pour ce faire, elles doivent s'assurer que les systèmes importants pour la sûreté respectent un haut niveau de fiabilité [16].

Dans cette optique, la Commission Canadienne de Sûreté Nucléaire (CCSN) exige la mise en œuvre de la norme d'application de la réglementation S-98, « Programme de fiabilité pour les centrales nucléaires » [16]. Cette exigence deviendra une condition au permis d'exploitation des centrales nucléaires canadiennes. La mise en œuvre du S-98 a pour but de s'assurer que les systèmes importants pour la sûreté (SIS) sont identifiés et que les détenteurs de permis ciblent leurs efforts sur ces systèmes de façon à maintenir un niveau de sûreté acceptable. L'objectif du programme de fiabilité exigé par la CCSN est de garantir la fiabilité des SIS en respectant leurs critères de conception, de performance et de sûreté [16]. Cet objectif étant atteint dès l'obtention d'un permis d'exploitation émis par la CCSN, la mise en oeuvre de la norme S-98 est réalisée davantage dans le but de s'assurer que les ressources et que les efforts permettant de maintenir un haut niveau de sûreté soient accordés aux SIS. L'identification des SIS et de leurs objectifs de fiabilité requière une attention particulière puisqu'ils définissent l'ensemble des systèmes qui seront soumis au programme de fiabilité exigé par la CCSN.

La démarche de la CCSN s'appuie sur une approche similaire entreprise aux États-Unis. En fait, la commission américaine responsable de la réglementation de l'industrie nucléaire (NRC) a senti le besoin d'identifier les systèmes ayant un impact significatif pour la sûreté de ses centrales nucléaires [32]. Aux États-Unis, les systèmes reliés à la sûreté (SRS) ne représentaient que les systèmes crédités dans les rapports de sûreté. Il pouvait donc exister des systèmes non-crédités possédant un impact significatif pour la sûreté. Une classification des systèmes a par conséquent été mise en branle en prenant en considération le niveau de risque présenté par chaque système de façon à identifier ceux considérés comme importants pour la sûreté.

Contrairement aux États-Unis, l'identification des SIS réalisée au Canada a eu pour effet de restreindre le nombre de systèmes critiques et ainsi concentrer les efforts. L'application de la norme S-98 constitue donc une évolution de ce qui est présentement utilisé par les centrales nucléaires canadiennes. Elle permettra d'identifier parmi tous

les SRS, ceux qui contribuent de manière significative à la sûreté de façon à leur accorder une attention particulière. L'exercice aura pour effet de concentrer les ressources pour les activités d'entretien, de surveillance, de suivi de la fiabilité opérationnelle, d'assurance qualité à l'approvisionnement, de gestion de la configuration, etc. afin d'assurer que la fiabilité des systèmes répond aux critères de conception, de performance et de sûreté pertinents.

L'évaluation de la sûreté des CANDU 600 est présentement réalisée grâce aux études déterministes, aux études matricielles de sûreté (ÉMS), aux études de fiabilité de certains systèmes et, pour certaines centrales, aux études probabilistes de sûreté (ÉPS) [22]. Les ÉMS ont été développées au Canada à la fin des années 1970. À cette époque, elles constituaient un avancement important en terme d'évaluation de la sûreté des centrales nucléaires [22]. Dans l'éventualité où les exploitants canadiens décident d'aller de l'avant avec les projets de réfection des centrales, des ÉPS devront être réalisées pour procéder à l'évaluation probabiliste de la sûreté des centrales nucléaires canadiennes.

1.2 Énoncé du problème

À l'heure actuelle, la réglementation canadienne ne détermine pas d'objectifs globaux de sûreté pour l'exploitation des centrales nucléaires [11]. Cependant, certains organismes internationaux ainsi que certaines centrales nucléaires canadiennes se sont dotés d'objectifs de sûreté. L'établissement des objectifs de fiabilité doit nécessairement se faire en accord avec les objectifs de sûreté fixés par les différentes installations.

Le critère de défaillance « Simple » précise que le nombre de défaillances majeures de procédé doit être inférieur à 0,3 défaillance par année tandis que celui pour la défaillance « Double » stipule qu'il doit y avoir moins d'une telle défaillance combinée à

l'indisponibilité d'un Système Spécial de Sûreté (SSS) par 3 000 ans. En se basant sur ce principe, les SSS sont donc les seuls systèmes à posséder un objectif de fiabilité réglementaire au Canada. Ce dernier est de 10E-03 année/année [13].

Les ÉMS et les études de fiabilité utilisées pour réaliser l'évaluation de la sûreté de certaines centrales CANDU 600 ne correspondent pas exactement à la nouvelle orientation internationale soit l'ÉPS [15].

Finalement, il n'existe pas de méthodologie directement applicable permettant de déterminer les objectifs de fiabilité des centrales nucléaires CANDU 600. Il s'avère indispensable de développer une telle méthodologie.

1.3 But et objectifs de l'étude

Le but de ce projet est de développer une méthodologie permettant d'identifier, de classer et d'attribuer les objectifs de fiabilité des SIS d'une centrale nucléaire de type CANDU 600 dont l'évaluation probabiliste de sûreté ne repose pas sur l'ÉPS. Ces objectifs devront être cohérents avec les objectifs de sûreté de la centrale nucléaire, les exigences en vigueur au Canada pour l'exploitation des centrales nucléaires ainsi que les recommandations internationalement reconnues. De plus, la méthodologie sera facilement compréhensible pour les décideurs et elle tiendra compte des forces et des faiblesses des techniques utilisées pour réaliser l'évaluation probabiliste de la sûreté de la centrale nucléaire.

Un des objectifs poursuivi par ce projet est de capturer le savoir non-documenté provenant d'experts en accordant une attention particulière à l'approche de prise de décision conservatrice.

1.4 Démarche et Portée

Cette étude porte sur le développement et la validation d'une méthodologie permettant de déterminer les objectifs de fiabilité d'une centrale nucléaire de type CANDU 600 dont l'évaluation probabiliste de la sûreté ne repose pas sur l'ÉPS. La méthodologie pourrait être applicable à des systèmes qui ne sont pas SIS mais qui remplissent tout de même une fonction de sûreté.

La méthodologie sera développée à partir d'informations disponibles concernant les centrales nucléaires CANDU 600 qui sont en exploitation depuis plus de 20 ans et ce, avec un bon dossier de sûreté. Elle sera fondée sur des connaissances documentées et tiendra compte du jugement d'experts qui permet de cerner certains facteurs intangibles.

La méthodologie sera définie en tenant compte des exigences pertinentes à l'exploitation des centrales nucléaires canadiennes. Elle sera développée en considérant les hypothèses de base émises lors de la réalisation des ÉMS et des études de fiabilité.

La méthodologie sera validée en calculant les objectifs de fiabilité d'un certain nombre de SIS identifiés à la seule centrale nucléaire exploitée par Hydro-Québec. Les systèmes choisis seront représentatifs des différentes classes de SIS. Les objectifs de fiabilité obtenus lors de la phase de validation de la méthodologie seront comparés à ceux d'autres centrales nucléaires CANDU 600 avec et sans ÉPS.

Les objectifs de fiabilité seront fixés seulement en considérant l'aspect de la sûreté. D'autres facteurs comme ceux économiques ne seront pas considérés. Cependant, il a été démontré que les centrales présentant un très bon bilan au niveau de la sûreté ne sont pas nécessairement moins performantes [25].

Ce rapport est composé de 6 chapitres. Voici une brève description du contenu de chacune des sections suivantes :

Chapitre 2 : Le chapitre 2 présente la revue de la littérature.

Chapitre 3 : Le chapitre 3 présente tous les éléments de la sûreté des centrales nucléaires à considérer pour le développement de la méthodologie.

Chapitre 4 : Le chapitre 4 présente la méthodologie développée.

Chapitre 5 : Le chapitre 5 présente les résultats de la validation de la méthodologie.

Chapitre 6 : Le chapitre 6 présente la conclusion et les recommandations.

CHAPITRE 2

REVUE DE LA LITTÉRATURE

Une revue exhaustive de la littérature a été réalisée afin de déterminer s'il existe une méthodologie permettant de déterminer les objectifs de fiabilité des centrales nucléaires de type CANDU 600, en particulier celles dont l'évaluation probabiliste de la sûreté n'est pas réalisée grâce à l'ÉPS. Cette démarche a été initiée dès le début du projet dans le but de ne pas développer une méthodologie déjà existante.

Voici deux objectifs poursuivis lors de cette phase:

- Comprendre les outils existants dans l'industrie nucléaire susceptibles d'aider à déterminer les objectifs de fiabilité (AMDEC, arbres de défaillance, etc.).
- Comprendre l'historique des objectifs de fiabilité des systèmes dans une centrale CANDU 600 au Canada et retracer les objectifs existants.

Plusieurs sources d'information ont été consultées lors de cette revue de la littérature : « Candu Owners Group » (COG), Agence Internationale de l'Énergie Atomique (AIEA), documentation interne d'Hydro-Québec, « United State Nuclear Regulatory Commission » (USNRC), Organisation de Coopération de Développement Économiques OCDE, « Massachusetts Institute of Technology » (MIT), standards militaires, l'Assocation Canadienne de Normalisation (CSA), la Société Nucléaire Canadienne (SNC), la Commission Canadienne de Sûreté Nucléaire (CCSN), « Electric Power Research Institute » (EPRI), etc. La revue a été réalisée selon les 3 critères de recherche suivants : Risque, Sûreté et Objectifs de fiabilité.

Voici une description des principaux éléments répertoriés pour chacun de ces éléments :

2.1 Risque

Puisque les objectifs de fiabilité doivent être déterminés de façon à s'assurer que la centrale présente un risque acceptable [16], il est nécessaire de bien comprendre le concept du risque.

Le risque peut être représenté comme étant le produit de la gravité des conséquences d'un accident et de la probabilité de leur occurrence [26]. L'acceptation du risque est soumise à plusieurs facteurs psychosociaux. De ce fait, il faut que la probabilité d'occurrence des dommages encourus soit inversement proportionnelle à la perception de la sévérité de ces dommages.

La perception du risque par la population doit être ajustée en fonction de sa nature [30]. En effet, les événements incontrôlables, catastrophiques et d'autres natures sont perçus de façon plus négative par la population que le risque qu'ils présentent vraiment.

La gestion du risque est un processus itératif global composé de plusieurs étapes qui permet d'établir le contexte, identifier, analyser, évaluer, maîtriser, suivre et communiquer les risques [10, 30, 33, 35]. Elle devrait faire partie intégrante des pratiques de gestion. Lorsqu'elle est appliquée de façon systématique, elle permet d'améliorer la prise de décision.

Plusieurs techniques permettent de procéder à l'analyse du risque [34, 35, 45]. Chacune possède des avantages et inconvénients ainsi qu'un domaine d'application particulier. L'Ordre des ingénieurs du Québec présente de façon détaillée les principales méthodes d'analyse du risque [35]. Ces dernières y sont par ailleurs très

bien expliquées. Voici une description sommaire des principales techniques répertoriées :

1- Étude des risques et de l'aptitude à l'exploitation (HAZOP) :

L'étude HAZOP est une technique qui a pour but d'identifier les dangers. Elle évalue toutes les parties d'un système afin de déterminer comment les déviations par rapport à la conception originale sont susceptibles de survenir et les problèmes qu'elles peuvent entraîner. Il s'agit d'un processus créatif qui est basé sur l'utilisation de mots-guides pour réaliser une recherche systématique des déviations [35]. La technique a initialement été développée pour les systèmes impliquant le traitement d'un milieu fluide ou autres flux de matières. Elle est maintenant utilisée dans plusieurs applications comme les logiciels, les systèmes de transport de personnes, l'examen des procédures d'exploitation, etc. Le déroulement d'une étude HAZOP se fait selon 4 phases : Définition, Préparation, Examen et Évaluation, Documentation. L'étude HAZOP est particulièrement efficace pour évaluer les systèmes thermo-hydrauliques. Il s'agit d'une bonne façon d'identifier les défaillances de cause commune mais ne permet pas d'évaluer les combinaisons de défaillances.

2- Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC)

L'AMDEC est une méthode inductive qui permet de réaliser une analyse qualitative de la fiabilité des systèmes. Elle a pour but d'évaluer l'impact ou la criticité de chacun des modes de défaillance sur la fiabilité, la maintenabilité, la disponibilité et la sécurité d'un système. Elle consiste à recenser les modes de défaillance, d'en évaluer les effets sur l'ensemble des fonctions du système et d'en analyser les causes. Elle est particulièrement efficace pour l'étude des défaillances simples. Elle est relativement exhaustive et elle permet d'identifier les défaillances de cause commune mais elle peut devenir très ardue à réaliser pour des systèmes complexes.

3- Analyse par arbre de défaillance

Un arbre de défaillance est une analyse déductive qui fournit une évaluation qualitative et quantitative du système [21]. Cette technique permet l'identification et l'évaluation de la probabilité d'occurrence d'un événement de tête. Elle est appuyée par une représentation graphique organisée des conditions ou des facteurs qui contribuent à l'avènement de l'événement indésirable [35]. Elle est particulièrement utile pour évaluer les systèmes possédant plusieurs sous-systèmes. La construction de l'arbre permet une compréhension des relations entre les systèmes. La principale information acquise par l'arbre de défaillance est la coupe minimale (minimal cutset). Une coupe est une combinaison d'événements de base qui cause l'événement de tête. Une coupe minimale est la plus petite combinaison d'événements de base qui résulte en l'apparition de l'événement de tête. Cette technique permet de cibler les maillons faibles d'un système. La réalisation de ce genre d'analyses requiert un analyste relativement expérimenté. La figure 1 présente un exemple d'arbre de défaillance.

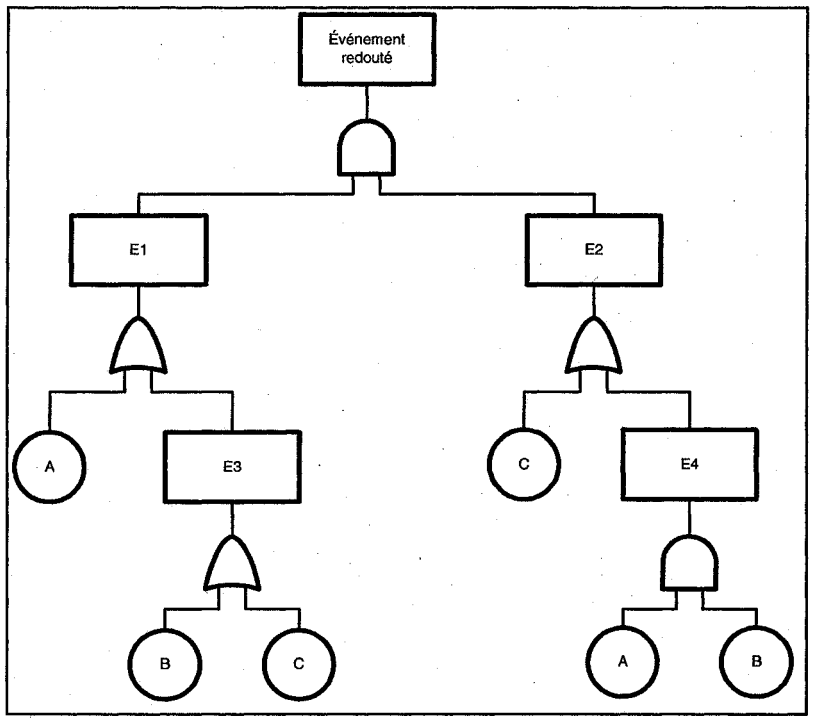


Figure 1 : Exemple d'arbre de défaillance [35]

4- Analyse par arbre d'événement

L'analyse par arbre d'événement emploie une méthode de raisonnement inductif qui étudie un événement initiateur de façon à déterminer la réponse de la centrale suite à son avènement. Elle tient compte de la réaction des différents systèmes de sûreté et de l'action de l'opérateur qui sont susceptibles d'atténuer les conséquences de l'événement [35]. Cette technique est appuyée par une représentation graphique qui permet de bien voir les séquences menant à des états indésirables. Elle requiert des ressources importantes. La figure 2 présente un exemple d'arbre d'événement.

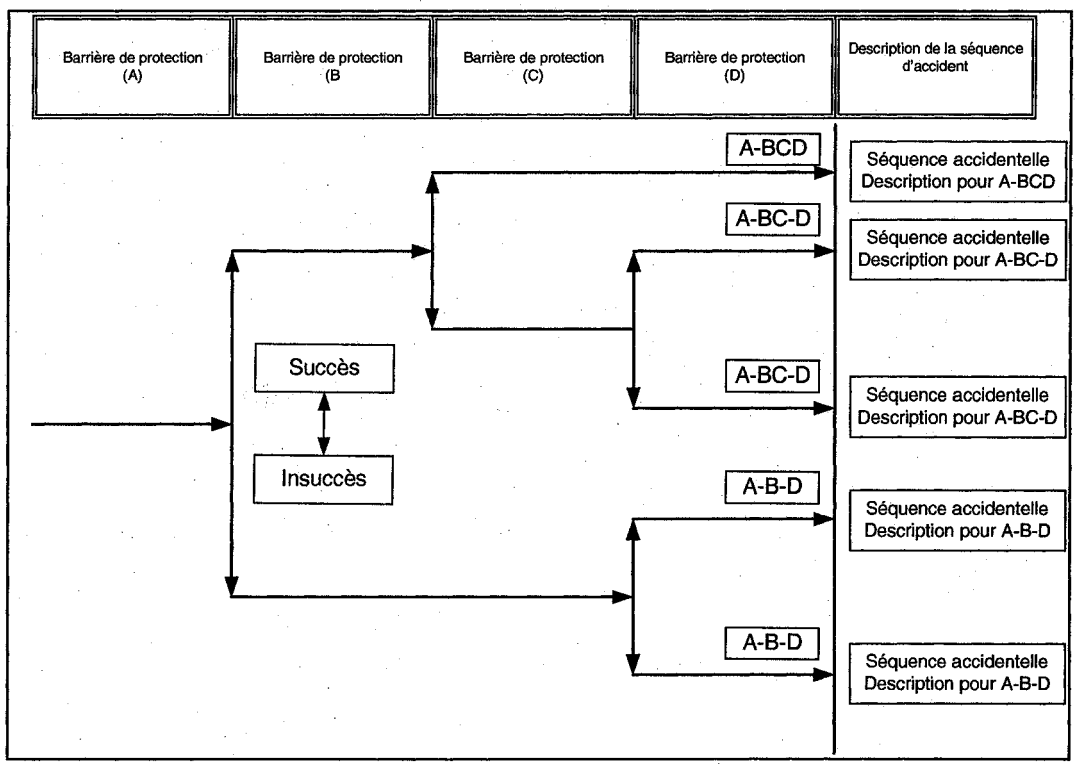


Figure 2 : Exemple d'arbre de d'événements [35]

5- Analyse préliminaire des dangers

L'analyse préliminaire des dangers est surtout utilisée dans la phase initiale de l'étude de sûreté d'un système. Elle permet de lister les dangers d'un système et d'en évaluer le risque résiduel suite à l'application des mesures d'atténuation. Elle inclut souvent la liste des mesures d'atténuation ainsi que la prédiction de leur efficacité [21]. Elle permet d'identifier les dangers les plus importants même si peu de données sont encore disponibles. Elle n'est pas très précise et c'est pourquoi elle est particulièrement utilisée lors des phases initiales d'un projet.

2.2 Sûreté

L'Agence Internationale de l'Énergie Atomique (AIEA) présente les principes fondamentaux qui assurent la sûreté des centrales nucléaires durant toutes les phases de leur cycle de vie [25].

Le principe de défense en profondeur est l'élément clé de la philosophie en matière de sûreté nucléaire [22]. Toutes les phases du cycle de vie des centrales nucléaires sont réalisées de façon à répondre à ce principe.

Une revue exhaustive des pratiques internationales a été réalisée concernant les objectifs de sûreté fondés sur le risque [38]. Elle présente les objectifs de sûreté établis par certains organismes de référence dans le domaine. Les résultats de cette revue sont présentés au chapitre 2.

Lors de la revue de la littérature, deux grandes approches d'évaluation de la sûreté des centrales nucléaires ont été identifiées. Il s'agit des analyses de type déterministe et probabiliste. Il a été identifié que cette dernière pouvait être réalisée par l'étude matricielle de sûreté (ÉMS), l'étude de fiabilité des systèmes et/ou l'étude probabiliste de sûreté (ÉPS).

2.3 Objectifs de fiabilité

Une méthodologie permettant de définir les objectifs de fiabilité lors de la conception de tuyaux d'un pipeline en fonction de l'analyse du risque a été identifiée [47]. L'objectif de fiabilité est obtenu en divisant le risque déterminé comme acceptable par les conséquences de la défaillance. La difficulté dans cette méthode réside à définir le niveau de risque acceptable. Ce dernier est fonction de la perception du public et est très difficile à évaluer.

Le CANDU Owners Group (COG), un regroupement d'exploitants de centrales nucléaires canadiennes, propose des pistes de solution permettant l'établissement des objectifs de fiabilité pour une centrale ne possédant pas d'ÉPS [11]. Voici les suggestions du COG pour un système de mitigation dont la défaillance ne constitue pas un événement initiateur :

- Dériver les objectifs à partir des ÉMS.
- Utiliser l'historique des données d'exploitation pour établir un objectif.
- Dériver les objectifs à partir des études de fiabilité.
- Utiliser les facteurs d'importance « Fussel-Vesely » (FV) et « Risk Achievement Worth » (RAW).

Voici les recommandations du COG pour les systèmes dont la défaillance constitue un événement initiateur :

- Dériver les objectifs à partir des ÉMS.
- Utiliser une ÉPS générique ou une ÉPS d'une autre centrale.
- Utiliser le jugement d'expert.
- Utiliser les données opérationnelles.

L'AIEA suggère des façons d'établir des critères en matière de sûreté pour les fonctions de sûreté et les systèmes [24]. La première approche décompose les objectifs de

sûreté globaux de la centrale en objectifs pour les systèmes. Cette technique requiert la présence d'une ÉPS complète de façon à pourvoir faire le lien entre le système et les exigences de sûreté de la centrale. Une autre façon de faire consiste à identifier une centrale ou un groupe de centrales qui possèdent une conception similaire et à utiliser les valeurs qu'elles ont établies mais il faut faire attention puisque les centrales ne sont pas parfaitement identiques.

Les objectifs de fiabilité sont généralement fixés à partir des expériences du passé, des standards de l'industrie, des besoins des clients ou d'un désir d'augmenter la fiabilité [20]. Les objectifs de fiabilité peuvent mener à un relâchement au niveau des efforts d'amélioration continue si les gens les considèrent comme étant atteints. Il faut donc considérer l'impact psychologique que peut entraîner l'établissement d'un objectif.

Certains éléments doivent être considérés pour déterminer les indicateurs de sûreté [41] :

1- Les objectifs doivent être significatifs, réalisables et gradués.
2- Les objectifs doivent être considérés comme un avertissement de la santé de la centrale et les limites acceptables doivent dépendre des valeurs fixées.
3- L'objectif doit tenir compte du statut de l'implantation des programmes.
4- Les objectifs doivent être révisés périodiquement.
5- Les objectifs doivent être réalisables par les ressources internes.
6- Les objectifs doivent contribuer à l'opération sécuritaire de la centrale.
7- Les objectifs doivent être fixés en fonction de l'expérience, de l'analyse et des spécifications techniques.

2.4 Revue de la revue de la littérature

Plusieurs documents ont été examinés afin de déterminer si une méthodologie pour déterminer les objectifs de fiabilité des SIS applicable à une centrale nucléaire CANDU 600 existait [7, 8, 9, 11, 20, 22, 23, 24, 25, 27, 28, 30, 31, 32, 38, 41, 42, 43, 44].

Malgré le fait que plusieurs éléments pertinents ont été identifiés, la revue de littérature n'a pas permis d'en découvrir. Il s'avère essentiel de développer une méthodologie pour déterminer les objectifs de fiabilité des centrales nucléaires CANDU 600 dont l'évaluation probabiliste de sûreté ne repose pas sur l'ÉPS.

Malgré le fait que la revue de la littérature n'a pas identifié la méthodologie recherchée, elle a tout de même identifié certains éléments importants à considérer pour son développement. Elle a aussi permis de déterminer les notions à approfondir pour être en mesure d'élaborer une méthodologie cohérente. Le tableau I présente une synthèse des techniques susceptibles de servir à l'élaboration de la méthodologie en fonction des principales approches d'évaluation de sûreté qu'elles utilisent.

Tableau I : Approches d'évaluation de la sûreté et techniques utilisées

Approches / Techniques	Étude déterministe de sûreté	Étude de fiabilité de système	ÉMS	ÉPS
Arbres de défaillance		X	X	X
Arbres d'événements			X	X
HAZOP				X
AMDE		X	X	X
AMDEC		X		X
Analyse préliminaire des dangers				X
Défaillance Simple/Double	X			

CHAPITRE 3

LA SÛRETÉ DES CENTRALES NUCLÉAIRES

La sûreté nucléaire peut être définie comme l'ensemble des techniques utilisées pour évaluer les risques inhérents des installations et pour les supprimer ou, à défaut, réduire leur probabilité d'apparition et l'importance de leurs conséquences à des niveaux acceptables aux termes de règlements existants ou suivant un consensus officiellement défini [36]. En fait, elle désigne toutes les mesures destinées à empêcher l'apparition de situations ou de conditions de fonctionnement pouvant menacer la sécurité des personnes ou du matériel par contamination radioactive, rayonnement ionisant ou par toute autre énergie libérée. La démarche entreprise pour déterminer les objectifs de fiabilité fait donc partie d'un ensemble d'activités ayant pour but d'assurer la sûreté des centrales nucléaires. Pour être en mesure de développer une approche cohérente, il est essentiel de bien comprendre en quoi elle consiste. Ce chapitre constitue une introduction à l'établissement des objectifs de fiabilité en faisant le point sur les notions entourant la sûreté des centrales nucléaires. Il est divisé en 5 grandes sections soit les principes de la sûreté, l'évaluation de la sûreté, les objectifs de sûreté, la gestion d'incident et les fonctions de sûreté.

3.1 Les principes de sûreté des centrales nucléaires.

La sûreté nucléaire représente l'ensemble des activités qui permettent de s'assurer que les installations sont exploitées à l'intérieur du risque défini comme acceptable. L'industrie nucléaire s'est donc dotée d'une série de principes de base qui servent de référence à l'ensemble des installations et qui permettent d'assurer un niveau global de sûreté. Ils sont énoncés sous forme d'objectifs généraux et de principes fondamentaux de sûreté. Ces principes s'inspirent directement du concept de gestion du risque détaillé à l'annexe A. Le tableau II présente un résumé des principes de sûreté. Tous ces éléments sont expliqués de façon plis détaillée à l'annexe B.

Tableau II : Objectifs généraux de sûreté, principes fondamentaux et spécifiques

Objectifs généraux de sûreté	Principes fondamentaux de gestion	Principes de défense en profondeur	Principes techniques généraux	Principes spécifiques
Objectif de sûreté général	Culture de sûreté	Prévention d'accident	Pratiques d'ingénierie reconnues	Site
Objectif de radioprotection	Responsabilité de l'exploitant	Atténuation de l'accident	Assurance qualité, auto évaluation et évaluation par les pairs	Conception
Objectif technique de sûreté	Vérification et contrôle réglementaire	Gestion de l'accident	Facteurs humains	Fabrication et construction
-	-	-	Évaluation de sûreté et vérification	Mise en service
-	-	-	Radioprotection	Exploitation
-	-	-	Retour d'expérience et recherche en sûreté	Gestion d'accident et mesures d'urgence
-	-	-	Excellence en exploitation	Déclassement

3.2 Évaluation de la sûreté des centrales nucléaires

L'établissement des objectifs de fiabilité est influencé directement par les techniques probabilistes utilisées dans l'évaluation de la sûreté d'une centrale nucléaire. La revue de la littérature a permis de déterminer qu'il existait deux grandes philosophies pour évaluer la sûreté des installations nucléaires soit l'approche déterministe et l'approche probabiliste [22]. Ces dernières sont associées à différentes techniques qui leur sont associées. L'annexe C les décrit de façon détaillée. De plus, elle fournit l'historique de

leur évolution au Canada et aux Canada. Ceci permet de situer la démarche entreprise par la CCSN concernant les programmes de fiabilité des centrales nucléaires canadiennes et particulièrement l'établissement des objectifs de fiabilité des SIS. Finalement, elle présente certaines hypothèses à la base de l'évaluation de la sûreté des centrales nucléaires.

3.3 Objectifs de sûreté

Les objectifs de fiabilité des systèmes doivent être cohérents avec les objectifs de sûreté de la centrale nucléaire de façon à ce que son exploitation soit réalisée à l'intérieur du risque défini comme acceptable. Il s'avère crucial de bien saisir ce que sont les objectifs de sûreté avant d'élaborer une méthodologie permettant de déterminer les objectifs de fiabilité des SIS. Cette section a pour but de présenter cette notion. Elle est divisée en 3 parties soit la définition du concept, sa portée ainsi que les recommandations internationales et exigences réglementaires pertinentes.

3.3.1 Définition du concept

Aux Canada, le « Nuclear Regulatory Commission » (NRC) a formulé des objectifs qualitatifs de sûreté qui stipulent que le risque pour la société provenant des centrales nucléaires devrait être comparable ou inférieur aux autres sources compétitives d'électricité. En fait, elles ne doivent pas augmenter de manière significative le risque par rapport à la population sans centrale nucléaire [38]. De façon à assurer la protection du public, le NRC a traduit ces objectifs qualitatifs en objectifs quantitatifs pour la santé [29]. Malgré le fait que ces objectifs ne font pas office de loi, ils font tout de même partie de l'énoncé de la politique de sûreté du NRC. Cette dernière stipule que l'exploitation d'une centrale nucléaire commerciale ne devrait pas augmenter le risque de mort subite d'un individu de plus de 0,1% et ne devrait pas entraîner une augmentation de cancers de plus de 0,1% par rapport à la population normale. Même si cette politique permet de déterminer de façon quantifiable le niveau de risque acceptable (« How safe is safe

enough ?»), il s'agit d'objectifs très généraux et il est difficile pour les centrales nucléaires de s'assurer qu'elles sont en mesure de les respecter. Des analyses de ce genre présentent trop d'efforts et d'incertitudes pour être valides. Dans le but de pouvoir assurer la sûreté des centrales nucléaires, ces objectifs ont été traduits en termes spécifiques pouvant être évalués plus facilement par les installations. Ces critères techniques correspondent aux objectifs de sûreté et sont exprimés sous la forme de probabilité de fonte du cœur et de probabilité de relâche importante de matières radioactives à l'extérieur du bâtiment réacteur (B/R). Ces derniers peuvent être évalués directement grâce à l'ÉPS.

3.3.2 Portée

Les objectifs de sûreté établis selon la probabilité de fonte du cœur et de relâche importante de matières radioactives à l'extérieur du B/R permettent d'évaluer le risque global d'une centrale nucléaire pour la population. Les événements internes et externes devraient être considérés dans l'analyse permettant d'évaluer le risque par rapport à ces deux critères. Même si une centrale nucléaire ne possède pas d'ÉPS, l'établissement des objectifs de fiabilité doit tout de même être réalisé en tenant compte de ces objectifs de sûreté.

3.3.3 Recommandations et exigences réglementaires

Au Canada, il n'y a pas d'objectifs de sûreté fixés par la réglementation canadienne. Cependant, l'industrie canadienne a adopté des objectifs en se basant sur ceux établis par des organismes reconnus dans le domaine nucléaire. Le tableau III présente les objectifs établis par ces organismes et par certaines centrales nucléaires canadiennes [38].

Tableau III : Objectifs de sûreté de différents organismes [38]

Organisme	Probabilité de fonte du cœur (par an)	Probabilité de relâche de produits radioactifs (par an)	Risque de mortalité subite	Risque du cancer
AIEA	10E-04	10E-05	-	-
NRC	10E-04	10E-05	Moins de 0,1% dû au nucléaire à l'intérieur d'un rayon de 1 mille.	Moins de 0,1% dû au nucléaire à l'intérieur d'un rayon de 10 milles.
OPG *	10E-05	10E-06**	-	-
Point Lepreau	10E-04	-	-	-
Hydro-Québec	10E-04	10E-05	-	-

Cible pour un risque moyen, ** Relâche importante

À noter que selon le directeur de la régulation des réacteurs nucléaires du NRC, les objectifs pour la santé se traduisent en un objectif pour la probabilité de fonte du cœur de 10E-02 par année [29]. Cependant, l'ensemble de l'industrie nucléaire américaine utilise un objectif pour la probabilité de fonte du cœur de 10E-04 par année. Cet écart s'explique par le fait que le NRC tente de protéger l'investissement économique que représente une centrale nucléaire contre les pertes potentielles d'un accident ainsi que les perceptions négatives de la population qui pourraient compromettre l'avenir de toute l'industrie. Cette situation permet donc d'assurer le respect des objectifs pour la santé de la population.

3.4 Gestion d'incident

La compréhension du processus de gestion d'un incident d'une centrale nucléaire de type CANDU permet de bien saisir les objectifs à atteindre pour stabiliser l'état de la

centrale suite à un incident et surtout de voir les systèmes qui y contribuent de manière significative. Cette section explique les différentes contraintes susceptibles de survenir suite à un incident, les objectifs génériques et les objectifs spécifiques que tente d'atteindre les opérateurs pour atténuer les conséquences. En plus de constituer une base au développement des séquences d'événement, la compréhension du processus de gestion d'incident permet d'identifier les diverses fonctions de sûreté et l'importance des différents systèmes requis pour les assurer.

3.4.1 Contraintes lors d'un incident

Certaines contraintes sont susceptibles de survenir lors d'un incident. Ces dernières peuvent nuire, voire même empêcher, les opérateurs et les systèmes d'atténuer les conséquences de l'incident de façon efficace. Un incident pourrait avoir un impact sur différents éléments participant à l'atténuation des conséquences comme l'arrêt du réacteur, l'habitabilité et l'accessibilité des salles de commande, le combustible dans la machine à chargement, le confinement et les fonctions de sûreté assurées par les systèmes du groupe 1 et 2. Suite à l'incident, l'opérateur doit donc travailler en fonction des différentes contraintes en présence.

Selon l'impact de l'incident, la centrale peut être stabilisée ou non. La centrale est considérée dans un état stable lorsque les fonctions de sûreté sont assurées adéquatement. Dans le cas contraire, le modérateur agit comme source froide ultime, la situation peut ne pas être couverte par une PEI ou encore il y a dégradation du cœur. Les caractéristiques de sûreté des CANDU présentées précédemment permettent de démontrer que la conception des centrales a été réalisée de façon à s'assurer que cette situation est improbable. La figure 3 présente les différentes contraintes susceptibles à considérer lors d'un incident.

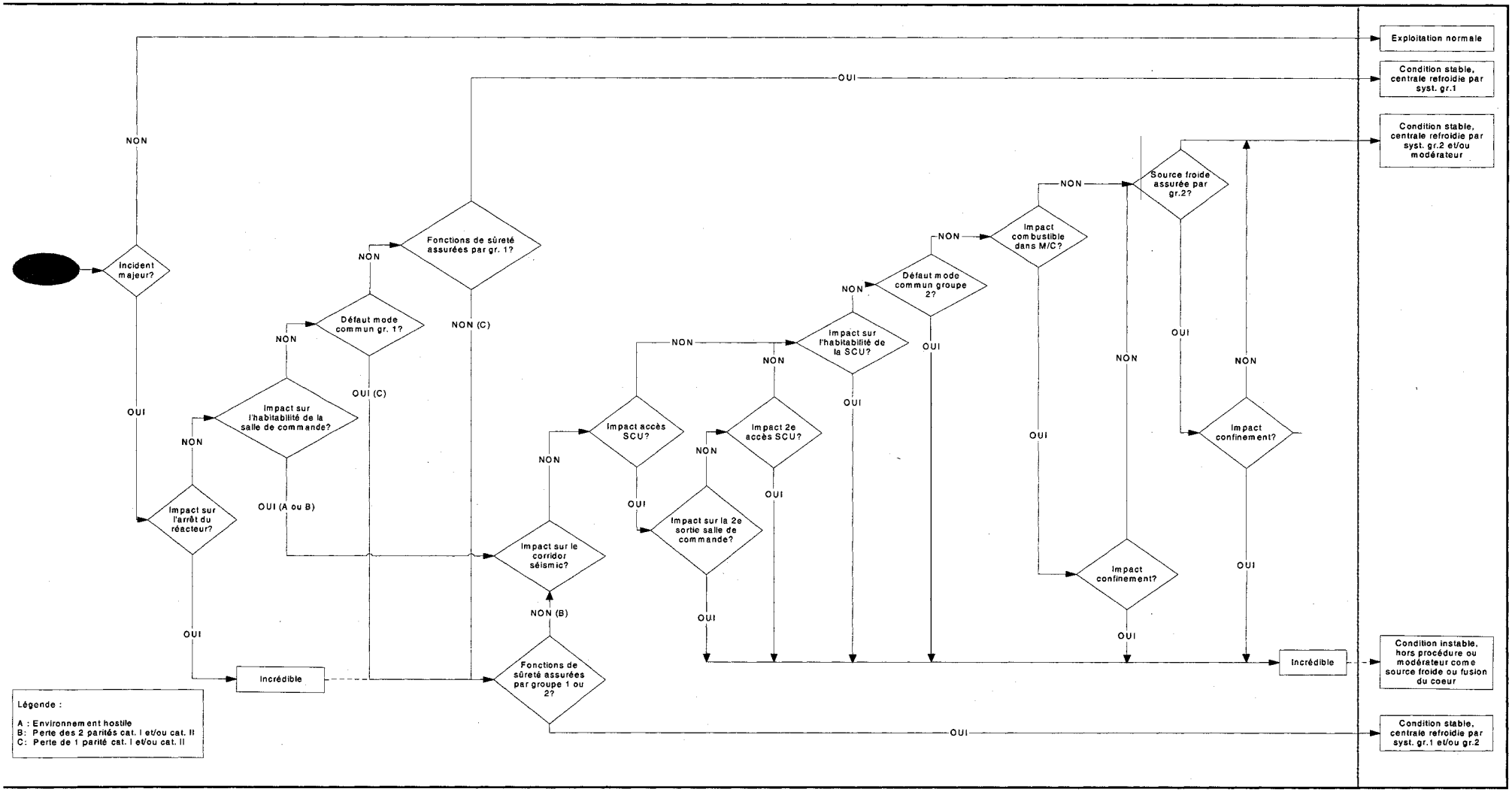
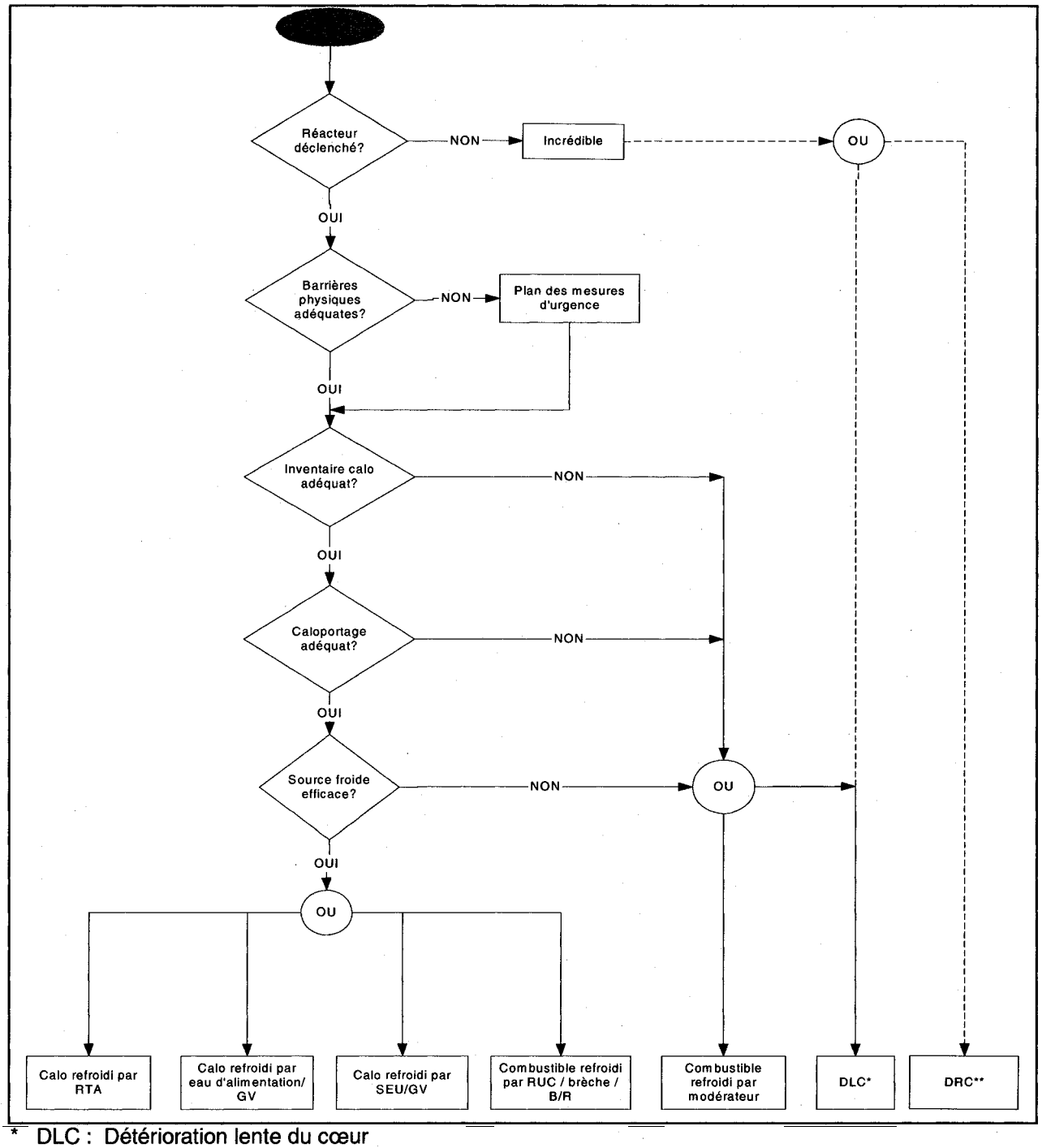


Figure 3 : Contraintes suite à un incident

3.4.2 Objectifs génériques suite à un incident

Il existe une série d'objectifs génériques que l'opérateur tente d'atteindre lors d'un événement afin de s'assurer que la centrale est mise dans un état stable. La première chose à se soucier lors d'un incident est l'arrêt du réacteur de façon à limiter la quantité d'énergie produite à évacuer. Ensuite, l'opérateur doit vérifier que les barrières physiques permettant d'assurer le confinement des matières radioactives sont efficaces. Il doit aussi s'assurer que l'inventaire de liquide caloporteur est suffisant pour évacuer la chaleur résiduelle du combustible. Pour la même raison, il doit veiller à ce que le liquide caloporteur circule de façon efficace et qu'une source froide adéquate soit disponible. Si tous ces éléments sont mis en place, la centrale est dans un état stable. La figure 4 présente les objectifs génériques.



* DLC : Détérioration lente du cœur

** DRC : Détérioration lente du Canada

Figure 4 : Objectifs génériques suite à un incident

3.4.3 Objectifs spécifiques suite à un incident :

De façon plus spécifique, chacun des objectifs génériques peut être assuré par certains systèmes. La figure 5 présente de façon générale les systèmes qui permettent à l'opérateur de stabiliser l'état de la centrale et l'ordre dans lequel ils sont susceptibles d'être sollicités. Cette schématisation permet de bien visualiser la façon dont seront développées les séquences d'événement.

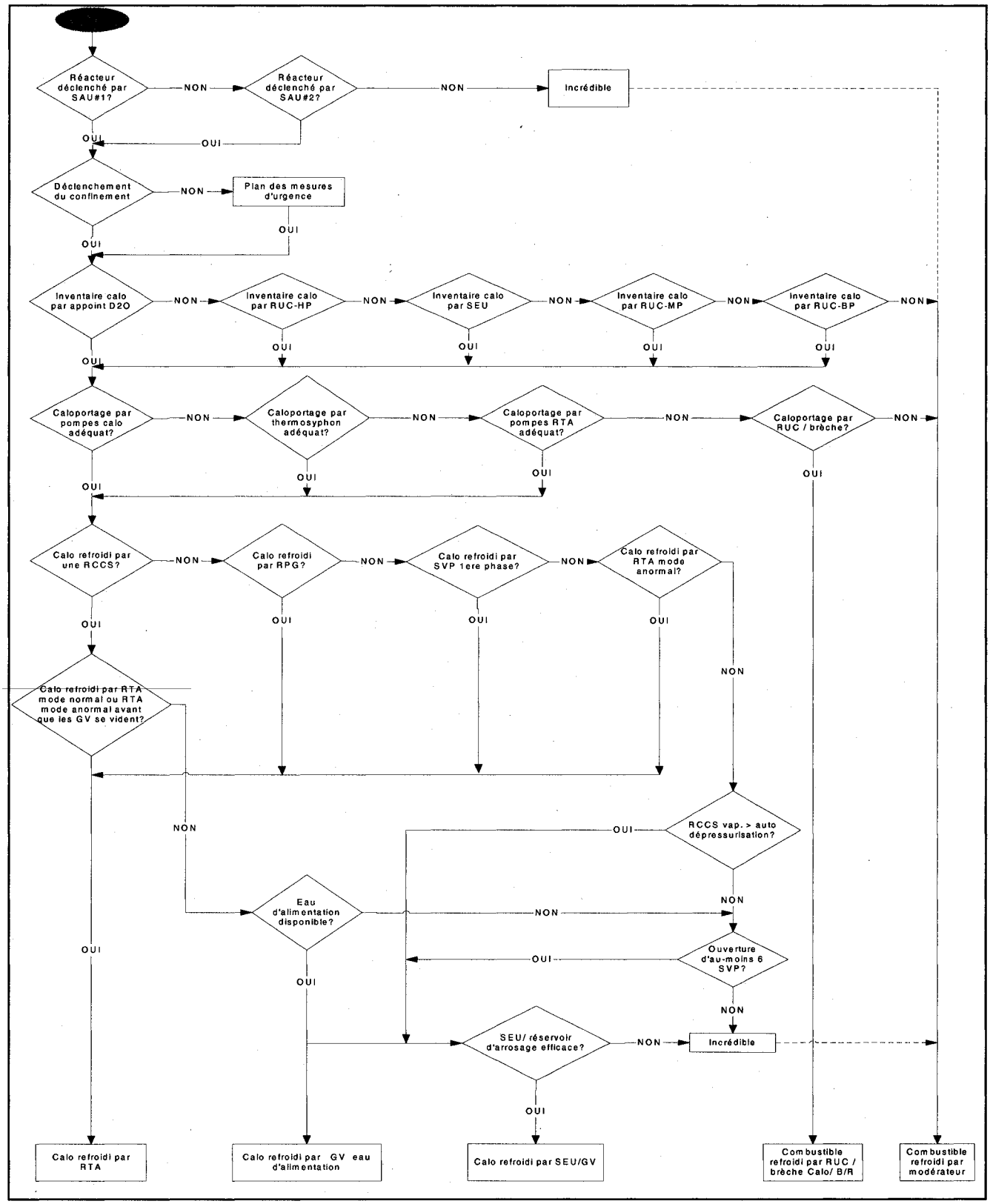


Figure 5 : Objectifs spécifiques

3.5 Fonctions de sûreté

Les systèmes identifiés comme importants pour la sûreté sont conçus pour assurer les principales fonctions de sûreté d'une centrale nucléaire. L'identification de ces dernières permettra de faciliter la compréhension du rôle joué par chacun des SIS, d'en évaluer l'importance et de déterminer un objectif de fiabilité en fonction du risque présenté par chacun des systèmes. La section précédente a permis de comprendre comment ont été identifiées les fonctions de sûreté en présentant les principaux éléments de la gestion d'incident. Dans le cadre de ce travail, il a été jugé pertinent de décomposer les 4 fonctions de sûreté principales généralement reconnues en sous-fonctions de sûreté. Le tableau IV présente les fonctions et sous-fonctions de sûreté identifiées.

Tableau IV : Fonctions et sous-fonctions de sûreté

Fonctions de sûreté	Sous-fonctions de sûreté
Arrêt du réacteur	Réduction de la puissance du réacteur
	Maintien de la sous-criticité
Confinement des produits radioactifs	Étanchéité du B/R
	Intégrité du B/R
	Abaissement du taux de fuite (abaisser la pression B/R)
	Maintien de l'intégrité de l'enveloppe du caloporteur
	Maintien de l'intégrité de l'enveloppe modérateur
	Maintien de l'intégrité du combustible
Refroidissement du combustible	Maintien de l'intégrité de l'enveloppe du caloporteur
	Maintien de l'inventaire primaire
	Circulation dans tous les canaux de combustible
	Contrôle de la pression du caloporteur
	Évacuation de la chaleur produite dans le caloporteur
	Maintien de l'inventaire des GV
	Refroidissement du fluide caloporteur
Surveillance et contrôle	-
Support aux systèmes	-

CHAPITRE 4

MÉTHODOLOGIE DÉVELOPPÉE

Ce chapitre présente la méthodologie développée pour déterminer les objectifs de fiabilité des SIS d'une centrale nucléaire CANDU 600 dont l'évaluation probabiliste de la sûreté ne repose pas sur l'ÉPS. Elle a été développée de façon à tenir compte de tous les principes de sûreté et des exigences réglementaires. Elle est inspirée de la nouvelle tendance dans l'industrie nucléaire qui consiste à prendre des décisions en utilisant la connaissance et la gestion du risque décrite à l'annexe A. La méthodologie est basée sur des techniques généralement reconnues et est fondée en partie sur le jugement d'experts. Il s'agit d'un processus où des valeurs préliminaires sont soumises à différentes phases de validation. Ces dernières ont été mises en place de façon à s'assurer que les objectifs de fiabilité répondront aux éléments pertinents identifiés dans les sections précédentes tels que les objectifs de sûreté, le risque présenté par les SIS, les prescriptions du « Siting Guide », les fonctions de sûreté, les valeurs des autres centrales canadiennes, etc. Tout au long du processus, la cohérence des résultats est validée par le jugement d'experts.

4.1 Étapes

La méthodologie développée se compose de 9 étapes :

1. Définir le concept d'objectif de fiabilité.
2. Recueillir les informations pertinentes concernant les SIS.
3. Évaluer la sévérité de la perte des fonctions de sûreté des SIS.
4. Déterminer une valeur préliminaire de l'objectif de fiabilité.
5. Évaluer la fréquence d'occurrence totale des défaillances majeures de procédé.
6. Développer des séquences d'événement et les évaluer par rapport aux objectifs de sûreté

7. Évaluer les arbres de défaillance des SIS de mitigation.
8. Compléter l'AMDEC des SIS, présenter leur criticité sur la matrice de risque et valider la cohérence des valeurs préliminaires.
9. Comparer avec les valeurs des autres centrales canadiennes.

La figure 6 présente le diagramme de processus de la méthodologie. Voici une description détaillée de toutes ses phases.

4.1.1 Définir le concept d'objectif de fiabilité

La première étape est de définir le concept d'objectif de fiabilité. Ceci permettre de déterminer des objectifs de fiabilité cohérents avec le contexte en vigueur dans la centrale où est réalisée l'application. Il s'agit de statuer sur ce qu'ils représentent, sur leur portée et sur les recommandations ou exigences réglementaires en vigueur au Canada. Cette étape est réalisée en tenant compte de tous les éléments de sûreté pertinents présentés au chapitre 2. Il s'agit d'une phase essentielle car elle définit le reste de la méthodologie.

4.1.2 Recueillir les informations pertinentes concernant les SIS

Cette étape permet de recueillir toute l'information nécessaire pour déterminer les objectifs de fiabilité des SIS. Les données recherchées sont les fonctions et les sous-fonctions de sûreté des SIS, les états de fonctionnement de la centrale considérés dans les études de fiabilité, les modes de défaillance des SIS, les valeurs en support au permis d'exploitation, les valeurs opérationnelles et les valeurs de conception. Toutes ces données sont nécessaires lors de l'application de la méthodologie.

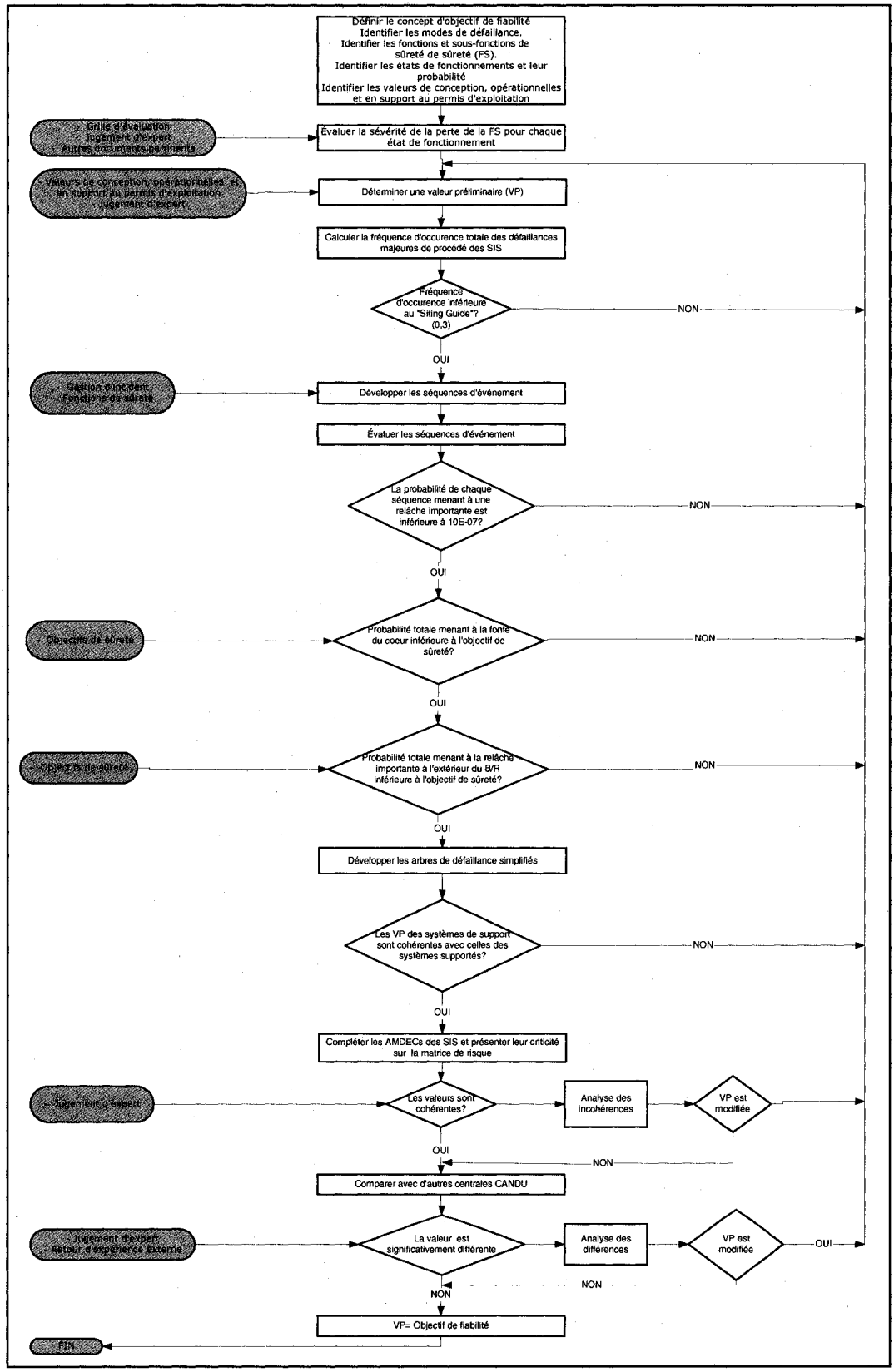


Figure 6 : Diagramme de processus de la méthodologie

4.1.3 Évaluer la sévérité de la perte des fonctions de sûreté des SIS

Pour chaque état de centrale, la sévérité de la perte des fonctions de sûreté assurées par les SIS est évaluée. Cette étape est un intrant majeur de la méthodologie puisqu'elle permet d'évaluer le risque présenté par chacun des systèmes. Cette évaluation est réalisée par jugement d'expert. Pour être en mesure de capturer tous les aspects de sûreté pertinents à considérer, l'évaluateur doit avoir une excellente connaissance du fonctionnement de la centrale. Pour cette raison, il est préférable que l'évaluation soit réalisée par un « Chef de quart ». Le processus de sélection et de formation pour ce type de personne est extrêmement rigoureux et requiert une connaissance très approfondie des systèmes contribuant à la sûreté de la centrale. L'évaluation est réalisée en considérant toute l'information disponible. Ceci permet d'assurer la qualité de l'évaluation. Afin de faciliter l'évaluation, une grille a été élaborée. Cette dernière contient des éléments clés permettant de juger l'importance des conséquences de la perte de la fonction de sûreté d'un système. Le tableau V présente cette grille. Elle constitue un outil servant à aider l'expert à porter un jugement concernant la sévérité d'un système. L'annexe E présente une explication de chacun des énoncés de la grille. Tous les systèmes sont soumis à la même grille et sont comparés selon cette base. Le processus d'évaluation doit être documenté de façon à mieux comprendre les raisons qui ont influencé le jugement de l'expert.

4.1.4 Déterminer une valeur préliminaire

En tenant compte des valeurs recueillies à l'étape 1, un expert en fiabilité de la centrale nucléaire détermine une valeur préliminaire de l'objectif de fiabilité pour les états de centrale considérés pour chaque SIS. La prise de décision est réalisée en considérant les valeurs en support au permis d'exploitation, les données opérationnelles, les données déterminées lors de la conception et les prescriptions réglementaires. Ces valeurs préliminaires sont validées dans les étapes suivantes.

4.1.5 Évaluer la fréquence d'occurrence des défaillances majeures de procédé

Les objectifs de fiabilité des systèmes de procédé représentent une fréquence d'occurrence d'événement. Le critère de défaillances « Simple » précise que la fréquence totale d'occurrence des défaillances majeures de procédé doit être inférieure à 3^{E}-01 par année. Il faut s'assurer que les valeurs préliminaires établies pour les SIS de procédé respectent ce critère.

Tableau V : Grille d'évaluation de la sévérité

#	Énoncé	Au prochain arrêt	Dans les mois qui suivent	Dans les jours qui suivent	Dans les heures qui suivent	Immédiatement
1	Quel est le délai de repli suite à la perte de la FS ?	0	5	10	20	40
	Énoncé	**Autres**	**Baisse de puissance (>2% PP)**	**BCP manuelle (< 2% PP)**	**Arrêt ordonné**	**SAU#1/SAU#2**
2	Quelle est l'action de repli suite à la perte de la FS ?	0	5	10	20	40
	Énoncé	**États de marche normale**	**Critique basse puissance**	**Sous-critique**	**Critique très basse puissance**	**EAG**
3	Quel est l'état de repli suite à la perte de la FS ?	0	5	10	20	40
	Énoncé	**-**	**Surveillance**	**Refroidissement**	**Confinement**	**Arrêt du réacteur**
4	Quelle est la fonction de sûreté ?	-	5	10	20	40
	Énoncé	**Ne s'applique pas**	**Peu**	**Moyen**	**Important**	**Critique**
5	La perte de la FS est susceptible de causer la défaillance d'autres SIS (cause commune) ?	0	5	10	20	40
6	La perte de la FS est susceptible de causer la défaillance de SRS (cause commune) ?	0	5	10	20	40
	Énoncé	**Très peu**	**Peu**	**Moyen**	**Beaucoup**	**Ne s'applique pas**
7	Il existe d'autres systèmes qui permettent de compenser la perte de la FS	40	20	10	5	0
	Énoncé	**Ne s'applique pas**	**Peu**	**Moyen**	**Important**	**Critique**
8	La perte de la FS entraîne la perte d'une ou plusieurs barrières de la défense en profondeur	0	5	10	20	40
	Énoncé	**Très peu**	**Peu**	**Moyen**	**Beaucoup**	**Ne s'applique pas**
9	Est-ce qu'une procédure permet à l'opérateur d'atténuer facilement les conséquences de la perte de la FS ?	40	20	10	5	0
	Énoncé	**Ne s'applique pas**	**Peu**	**Moyen**	**Important**	**Critique**
10	Est-ce que la perte de la FS réduit la capacité de l'opérateur à prendre des décisions permettant d'atténuer les conséquences de l'événement ?	0	5	10	20	40
11	La perte de la FS est susceptible d'entraîner des doses aux travailleurs, et/ou à l'environnement, et/ou au public	0	5	10	20	40

4.1.6 Développer des séquences d'événement et les évaluer par rapport aux objectifs de sûreté

Le développement de séquences d'événement permet de s'assurer que les valeurs préliminaires sont cohérentes avec les objectifs de sûreté de la centrale. Le choix des scénarios étudiés est laissé au jugement d'un expert en fiabilité. Cette décision consiste en un compromis entre les gains à ajouter un scénario particulier et les efforts requis. Les arbres d'événement doivent être développés en considérant les éléments pertinents de la gestion d'incident présentés au chapitre 2. Seuls les SIS sont représentés dans les arbres d'événement pour atténuer les conséquences de l'incident. Cette approche est donc conservatrice puisqu'elle ne considère pas les autres systèmes qui pourraient contribuer à diminuer les effets néfastes. Chaque séquence menant à la relâche de matières radioactives à l'extérieur du B/R doit être négligeable c'est-à-dire avoir une probabilité d'occurrence inférieure à 10^{E}-07. Les fréquences totales de fonte du cœur ou de relâche importante à l'extérieur du B/R doivent être inférieures aux objectifs de sûreté. La fréquence de fonte du cœur est évaluée en additionnant la valeur de toutes les branches de l'arbre qui mènent en une indisponibilité du modérateur comme source froide ultime et de celles où le réacteur n'est pas arrêté. La fréquence d'occurrence de relâche importante à l'environnement est évaluée en calculant la valeur totale de toutes les branches de l'arbre qui mènent en une indisponibilité du modérateur comme source ultime. Cette dernière est multipliée par la probabilité que le confinement soit indisponible. Finalement, il faut ajouter la somme des branches où le réacteur n'est pas arrêté. Dans le cas où un de ces 3 critères ne serait pas respecté, les valeurs préliminaires sont réévaluées.

4.1.7 Évaluer les arbres de défaillance des SIS de mitigation.

L'évaluation via les arbres d'événement permet de s'assurer que l'utilisation des systèmes de mitigation respecte les objectifs de sûreté de la centrale. Ces évaluations ne démontrent pas l'importance des systèmes de support. Afin de s'assurer de la cohérence de valeurs préliminaires des systèmes de support, il faut les intégrer aux arbres de défaillance des SIS de mitigation. Ces derniers doivent être en mesure de

respecter leur objectif de fiabilité en tenant compte des valeurs préliminaires fixées pour les systèmes de support. Des arbres de défaillance simplifiés peuvent être développés pour les systèmes de mitigation qui ne possèdent d'arbres de défaillance.

4.1.8 Compléter l'AMDEC des SIS, présenter leur criticité sur la matrice de risque et valider la cohérence des valeurs préliminaires.

Toutes les étapes précédentes de la méthodologie consistent à réunir et à valider l'information nécessaire pour évaluer la criticité des SIS selon la méthode de l'AMDEC. Une fois les AMDEC des SIS complétées, les SIS sont présentés sur la matrice du risque. Cette dernière montre tous les SIS par rapport au niveau de risque qu'ils présentent pour la centrale. Un système ne doit pas présenter un risque inacceptable pour un état de fonctionnement donné. Les SSS servent de base de comparaison puisqu'ils ont un objectif de fiabilité fixé par la réglementation. Ils définissent le risque acceptable. Les SIS ayant le même niveau de sévérité devraient normalement présenter un risque équivalent. Ils devraient par conséquent posséder un objectif de fiabilité situé dans le même ordre de grandeur. La matrice de risque utilisée est inspirée des standards militaires [18]. Les tableaux VI, VII et VIII présentent respectivement les catégories de probabilité, de sévérité et de risque tandis que le tableau IX montre la structure de la matrice.

Tableau VI : Catégories de probabilité

#	Description	Intervalle
1	Fréquent	$10E\text{-}02 < X \leq 1$
2	Probable	$10E\text{-}03 < X \leq 10E\text{-}02$
3	Occasionnel	$10^{E}\text{-}04 < X \leq 10^{E}\text{-}03$
4	Rare	$10E\text{-}05 < X \leq 10E\text{-}04$
5	Improbable	$X \leq 10^{E}\text{-}05$

Tableau VII : Catégories de sévérité

#	Description	Intervalle
1	Critique	$330 < Y \leq 440$
2	Important	$220 < Y \leq 330$
3	Marginal	$110 < Y \leq 220$
4	Négligeable	$0 < Y \leq 110$

Tableau VIII : Catégories de risque

Catégorie de risque	Évaluation du risque
Sérieux	
Élevé	
Moyen	Jaune
Bas	

Tableau IX : Matrice de risque

Sévérité / Probabilité	Négligeable	Marginal	Important	Critique
Fréquent				
Probable				
Occasionnel				
Rare				
Improbable				

4.1.9 Comparer les valeurs préliminaires avec les objectifs de fiabilité des autres centrales nucléaires canadiennes

Cette étape consiste à déterminer s'il existe une différence significative entre les valeurs préliminaires de la centrale nucléaire et les objectifs de fiabilité fixés par les autres centrales nucléaires canadiennes. S'il est déterminé qu'une valeur préliminaire présente un écart jugé significatif, une analyse est réalisée afin de voir si des modifications doivent être effectuées. Une fois cette étape complétée, les valeurs préliminaires sont considérées comme les objectifs de fiabilité des SIS.

4.2 Avantages

Voici les avantages que présente la méthodologie développée :

1- La méthodologie s'inscrit dans la ligne de pensée de la prise de décision utilisant la connaissance du risque puisqu'elle considère plusieurs intrants autant quantitatifs que qualitatifs pour la prise de décision :

   - Sévérité de la perte de la fonction du SIS;
   - Fonctions et sous-fonctions de sûreté;
   - Risque selon les états de fonctionnement et leur probabilité;
   - Objectifs de fiabilité des autres centrales CANDU;
   - Objectifs de sûreté;
   - Prescriptions réglementaires, « Siting Guide », etc.;
   - Valeurs de conception, opérationnelles, en support au permis, et;
   - Principes fondamentaux de sûreté.

2- L'utilisation du jugement d'expert permet de considérer des facteurs intangibles comme l'intuition, l'impact humain, l'impact organisationnel, la dynamique du quotidien, etc.

3- Les SSS sont utilisés comme référence pour déterminer le niveau de risque acceptable puisqu'ils possèdent déjà un objectif de fiabilité. Les autres SIS peuvent être comparés par rapport aux SSS via la matrice du risque.

4- Les objectifs de fiabilité des SIS sont comparés entre eux et ensuite comparés à ceux d'autres centrales de type CANDU.

5- La pondération de la grille d'évaluation des conséquences n'est pas critique puisque tous les SIS sont comparés entre eux selon cette même grille. De plus, l'expert s'assure que son évaluation est la plus représentative possible.

6- Un objectif de fiabilité peut être fixé même pour un SIS qui ne possède pas d'étude de fiabilité ou qui n'est pas crédité dans une étude matricielle de sûreté.

8- L'objectif de fiabilité est fixé selon les états de fonctionnement de la centrale considérés dans les études de fiabilité. Les objectifs pourront directement être comparés à celles présentes dans les études.

9- La méthodologie est composée de nombreuses phases de validation qui ont été intégrées en fonction des éléments jugés essentiels à considérer pour l'établissement des objectifs de fiabilité.

10- La méthodologie est basée sur des techniques généralement reconnues : AMDEC, prise de décision en connaissance du risque, matrice du risque, arbres de défaillances, arbres d'événement, etc.

11- La méthodologie est flexible. Tout peut-être adapté en fonction du jugement d'expert. De plus, il s'agit d'un processus itératif qui comprend des retours en arrière si nécessaire.

12-La méthodologie est relativement simple à appliquer et ne demande pas une trop grande charge de travail.

13-La méthodologie pourrait être applicable à d'autres systèmes qui ont un rôle au niveau de la sûreté de la centrale.

14-La méthodologie fait appel à un groupe d'experts. Par conséquent, l'établissement des objectifs de fiabilité tient compte de plus d'un point de vue. Les experts travaillent d'abord de façon individuelle sur certains aspects spécifiques de la méthodologie. Ensuite, les résultats sont présentés au groupe pour validation.

15-La méthodologie ne requiert pas d'ÉPS.

4.3 Inconvénients

1- La méthodologie demande un expert possédant une très grande connaissance du fonctionnement de la centrale pour évaluer la sévérité de chaque système. Il est essentiel d'avoir un « Chef de quart » ayant été autorisé par la CCSN. Il est plutôt difficile d'obtenir cette ressource puisque compte tenu de leur expertise, ils sont très sollicités.

2- La même personne est requise pour évaluer la sévérité de chaque système de façon à ce que les résultats soient cohérents entre les systèmes.

3- Compte tenu des ressources disponibles, l'analyse de sensibilité de la grille d'évaluation avec différents évaluateurs n'a pu être réalisée. Cependant puisque la grille se base sur plusieurs éléments documentés, la variabilité entre les différents experts ne devrait pas être trop grande.

4- La méthodologie n'est pas entièrement quantitative, elle laisse place aux intuitions et au jugement des experts.

5- Il s'agit d'une approche simplifiée puisque seulement certains scénarios sont évalués à la discrétion d'un expert en fiabilité. Ils peuvent permettre de confirmer l'ordre de grandeur des objectifs de fiabilité par rapport aux objectifs de sûreté de la centrale. Cependant, ils ne représentent pas l'ensemble des risques présents dans une centrale nucléaire et ne sont pas aussi précis qu'une ÉPS.

6- La méthodologie est relativement spécifique à l'industrie nucléaire et serait difficilement adaptable à d'autres industries.

7- La méthodologie tient compte des contraintes présentes dans les centrales nucléaires CANDU 600 ne possédant pas d'ÉPS. Elle est donc spécifique à ce type de centrales.

8- La méthodologie sera adaptée lorsque l'évaluation de la sûreté sera réalisée par une ÉPS.

CHAPITRE 5

VALIDATION DE LA MÉTHODOLOGIE DÉVELOPPÉE

La méthodologie présentée au chapitre précédent a été validée en l'appliquant à un nombre de SIS d'une centrale nucléaire exploitée par Hydro-Québec. L'annexe E présente la méthodologie utilisée pour identifier les SIS de cette centrale, les grandes classes de SIS et une brève description des systèmes sélectionnés dans le groupe utilisé pour la validation. À noter que les travaux concernant l'identification des SIS dans cette centrale ne sont pas encore terminés. Les systèmes présentés dans ce rapport sont donc susceptibles d'être supprimés de la liste des SIS et d'autres systèmes peuvent s'y ajouter. Les SIS utilisés pour la validation ont été sélectionnés par Hydro-Québec de façon à ce que chaque grande classe de SIS soit représentée par au-moins un système. En fait, seule la « Surveillance » ne fait pas partie du groupe puisque les évaluations nécessaires ne sont pas encore toutes complétées. Les SIS pour lesquels la méthodologie a été appliquée sont le système de Refroidissement d'Urgence du Cœur (RUC), le Système d'eau d'Urgence (SEU), l'Eau de Service Re-circulée (ESR), le caloporteur et le modérateur. Les différentes phases de la méthodologie sont appliquées à ce groupe comme s'il constituait l'ensemble des SIS de la centrale sauf pour les arbres d'événement. En effet, il n'est pas possible d'évaluer ce critère de décision sans avoir recours à l'ensemble des SIS. Les valeurs déterminées lors de cette validation ne sont pas nécessairement celles qui seront obtenues lorsque la méthodologie sera appliquée de façon systématique à l'ensemble des SIS. Voici les résultats de la méthodologie appliquée au groupe de SIS identifiés.

5.1 Définir le concept d'objectif de fiabilité.

Afin de préciser le concept d'objectif de fiabilité, un questionnaire a été élaboré et envoyé à des experts de la centrale nucléaire. Ces derniers ont été sélectionnés selon la nature de leur expertise. Cette façon de procéder a permis de capturer une partie du

savoir non-documenté de ces personnes. L'annexe F présente le questionnaire. Les parties qui suivent concernant les objectifs de fiabilité sont donc directement inspirées des réponses de ces experts au questionnaire.

5.1.1 Définition du concept

L'objectif permet de s'assurer que le risque présenté par le système est acceptable en considérant la prévention et l'atténuation des accidents et ce dans un contexte économique compétitif, tout en respectant de bonnes pratiques d'ingénierie [13]. Il doit être en accord avec les objectifs de sûreté de la centrale.

L'objectif de fiabilité des systèmes de mitigation est défini par la probabilité que le système soit disponible au moment où il est sollicité et qu'il fonctionne pendant le temps requis. L'objectif de fiabilité de ces systèmes est fonction de leur disponibilité et de leur fiabilité. Les systèmes de procédé sont plutôt considérés comme des événements initiateurs. Leur objectif de fiabilité représente une fréquence d'occurrence d'événements par année. Pour un système donné, il y peut y avoir plus d'un objectif de fiabilité. En fait, l'objectif doit être fixé de façon à tenir compte des différents modes de défaillance du système et des états de fonctionnement considérés dans les études de fiabilité [13].

5.1.2 Portée

Les objectifs de fiabilité sont nécessaires pour démontrer que la fiabilité postulée répond aux exigences de conception. Les objectifs de fiabilité toucheront principalement trois parties intéressées soit le titulaire du permis, l'organisme réglementaire et l'exploitant. Le premier les utilisera pour s'assurer que son installation respecte le dimensionnement et les conditions du permis en révisant les indicateurs de performance et de disponibilité. Le second s'assura que les objectifs de fiabilité respectent les conditions au permis d'exploitation et il vérifiera que le titulaire du permis les respecte. Finalement, l'exploitant confirme la disponibilité des systèmes en réalisant les essais et en appliquant les actions, délais et états de repli.

L'objectif de fiabilité ne représente pas une limite qui, lorsqu'une fois franchie, entraîne nécessairement des conséquences néfastes pour la santé du public. Il se veut davantage un intrant permettant d'évaluer le niveau de défense en profondeur. Il facilite la prise de décision concernant les actions à entreprendre de façon à respecter les exigences du dimensionnement. L'objectif de fiabilité se veut une information supplémentaire à la prise de décision en utilisant la connaissance du risque. En outre, il devrait être un intrant important à la prise de décision sur perte ou lors d'un retrait volontaire d'un composant redondant.

L'objectif de fiabilité sera révisé lorsque de nouvelles informations seront connues comme des changements au niveau des valeurs opérationnelles ou encore lorsque des modifications physiques devront être apportées [13]. Par exemple, l'objectif pourrait être modifié lorsqu'un système est utilisé pour compenser la déficience d'un autre système dans le cas d'une situation bien précise. Les objectifs de fiabilité sont évalués en fonction des scénarios étudiés lors des révisions des études de fiabilité.

Le titulaire du permis s'assure qu'il respecte les objectifs de fiabilité en réalisant des études de fiabilité et en calculant l'indisponibilité des systèmes sur une base annuelle. Pour les systèmes de procédé, le titulaire du permis dénombre toutes les défaillances majeures de procédé survenues lors des trois dernières années pour s'assurer qu'il respecte le critère de défaillance « Simple ».

Lors d'une prise de décision sur perte ou lors d'un retrait volontaire d'un composant redondant, le titulaire du permis devrait s'assurer que l'objectif de fiabilité est respecté sur une base annuelle. Pour ce faire, il considère toutes les heures d'indisponibilité à partir du début de l'année, de celles prévues pour la perte ou le retrait ainsi que toutes celles programmées jusqu'à la fin de l'année. Ces dernières tiennent compte de l'indisponibilité moyenne passée du système et des autres indisponibilités prévues pour comme les entretiens. Cette analyse est établie par un expert en fiabilité.

Une série d'actions est entreprise lors du dépassement d'un objectif de fiabilité. Premièrement, un rapport de condition anormale (RCA) est émis afin qu'un processus de suivi soit mis en place à l'interne. Ensuite, une analyse est réalisée pour déterminer si la situation représente un risque acceptable pour la centrale et qu'elle respecte les exigences réglementaires en vigueur. L'objectif de fiabilité sera réévalué si l'analyse en démontre la pertinence. Un plan d'actions est élaboré afin de déterminer les actions à mettre en branle afin de remédier à la situation. La centrale nucléaire avertit la CCSN de cette condition via le rapport annuel de fiabilité. Elle justifie la situation et explique ce qu'elle entend faire pour y remédier. Le titulaire du permis signale à la CCSN toutes modifications apportées aux objectifs de fiabilité et en expliquer les raisons.

5.1.3 Recommandations et exigences réglementaires

Au Canada, seuls les SSS ont un objectif de fiabilité exigé par la CCSN. En effet, les Systèmes d'Arrêt d'Urgence (SAU#1, SAU#2), RUC et confinement ont un objectif réglementaire de 10^{E}-03 année/année. De plus, l'objectif pour toutes les défaillances majeures de procédé stipule qu'il doit y avoir moins d'une de ces défaillances par 3 ans.

5.2 Recueillir les informations pertinentes concernant les SIS.

Les informations recherchées serviront principalement à établir la criticité des systèmes selon la technique de l'AMDEC. Les fonctions et les sous-fonctions de sûreté, les modes de défaillance, les états de fonctionnement sont les éléments essentiels pour réaliser l'évaluation des SIS. Les valeurs opérationnelles, de conception et en support au permis sont aussi recueillies pour permettre à l'expert en fiabilité de déterminer des valeurs préliminaires cohérentes. Voici les principales informations recueillies :

5.2.1 Les fonctions de sûreté des SIS

Les fonctions et les sous-fonctions de sûreté assurées par chacun des SIS du groupe sélectionné ont été identifiées en considérant les éléments relatifs à la gestion d'incidents présentés au chapitre 2. Le tableau X présente les fonctions des SIS.

Tableau X : Fonction et sous-fonctions de sûreté des SIS

SIS	Fonctions de sûreté	Sous-Fonctions de sûreté
RUC	Confinement des produits radioactifs	Intégrité du B/R
	Refroidissement du combustible	Maintien de l'inventaire primaire
		Refroidissement du fluide caloporteur
		Circulation dans tous les canaux de combustible
		Contrôle de la pression du caloporteur
		Évacuation de la chaleur produite dans le caloporteur
		Maintien de l'inventaire des GV
Modérateur	Confinement des produits radioactifs	Étanchéité du B/R
		Maintien de l'intégrité de l'enveloppe du modérateur
	Arrêt du réacteur	Maintien de la sous-criticité
	Refroidissement du combustible	Évacuation de la chaleur produite dans le caloporteur
SEU	Refroidissement du combustible	Maintien de l'inventaire primaire
		Maintien de l'inventaire des GV
	Confinement des produits radioactifs	Étanchéité du B/R
Caloporteur	Confinement des produits radioactifs	Étanchéité du B/R
		Maintien de l'intégrité de l'enveloppe du caloporteur
	Refroidissement du combustible	Maintien de l'inventaire primaire
		Circulation dans tous les canaux de combustible
		Évacuation de la chaleur produite dans le caloporteur
		Maintien de l'inventaire des GV
		Refroidissement du fluide caloporteur
ESR	Support aux systèmes	-

5.2.2 Modes de défaillance des SIS

Les modes de défaillance de chacun des SIS du groupe sélectionné ont été identifiés. Le tableau XI présente ces modes de défaillance des systèmes.

Tableau XI : Modes de défaillance des SIS

SIS	Modes de défaillance
RUC	- Incapacité à détecter une situation requérant l'initiation automatique du RUC
	- Incapacité à détecter une situation requérant l'isolation automatique des boucles du caloporteur
	- Incapacité à fournir le débit requis pour le fonctionnement efficace du RUC-HP
	- Incapacité à isoler le RUC-HP après son injection
	- Incapacité de procéder à l'isolation de la boucle intacte lorsque requis
	- Incapacité d'assurer le refroidissement ultra-rapide des GV
	- Incapacité à fournir le débit requis pour le fonctionnement efficace du RUC-MP
	- Incapacité de réaliser le passage manuel du RUC-MP vers le RUC-BP
	- Incapacité à fournir le débit requis pour le fonctionnement efficace du RUC-BP
	- Incapacité à fournir le débit requis au secondaire de l'échangeur du RUC
SEU	- Incapacité d'alimenter l'eau d'urgence aux GV
	- Incapacité d'alimenter l'eau d'urgence au secondaire de l'échangeur du RUC
	- Incapacité d'alimenter l'eau d'urgence au caloporteur
	- Incapacité d'alimenter l'eau d'urgence simultanément au secondaire de l'échangeur du RUC et aux GV
ESR	- Incapacité d'assurer le refroidissement des charges de l'ESR
	- Incapacité de procéder à la relâche de charges lors d'une perte de catégorie IV
	- Incapacité de démarrer les pompes de relève ESR lors d'une perte de catégorie IV
	- Incapacité d'assurer un refroidissement de relève aux systèmes essentiels suite à une perte d'ESR
Caloporteur	- Incapacité d'assurer le refroidissement adéquat du combustible (centrale à 100% P.P.)
	- Incapacité d'assurer le refroidissement adéquat du combustible (réacteur à l'arrêt, caloporteur chaud et pressurisé) avec les GV comme source froide
	- Incapacité d'alimenter les GV suite à une perte de cat. 4
	- Incapacité d'assurer le refroidissement du système caloporteur par dépressurisation des GV
Modérateur	- Incapacité à évacuer la chaleur normalement transmise par le combustible au modérateur
	- Incapacité à assurer le refroidissement du combustible comme source froide ultime dans le cas d'une PERCA combinée à une indisponibilité du RUC
	- Incapacité à assurer un milieu adéquat à l'efficacité du SAU#2 et au maintien de la sous-criticité par poisons solubles

5.2.3 États de fonctionnement

La probabilité que la centrale se retrouve dans un état donné a été évaluée à partir de documents internes d'Hydro-Québec. Le tableau XII présente les valeurs considérées pour l'étude.

Tableau XII : Probabilité des diverses situations d'incident

Situation	Probabilité
Centrale en puissance	8,30E-01
Centrale à l'arrêt	1,70E-01
Petite PERCA	1,00E-02
Grosse PERCA	1,00E-03
SDE	1,00E-02
DBE	1,00E-03
Petite PERCA suivie d'un SDE 24 heures après	1,00E-04
Grosse PERCA suivie d'un SDE 24 heures après	1,00E-05
Situation d'urgence	1,00E-01

Compte tenu des ressources limitées, l'évaluation de la sévérité d'un système ne peut être réalisée de façon indépendante pour toutes les situations susceptibles de survenir. Pour cette raison, la catégorie « Situation d'urgence » a été instaurée avec une probabilité relativement conservatrice de 0,1. Elle peut notamment comprendre une perte de catégorie 4, une haute pression dans le B/R, une haute activité dans le B/R, etc. L'évaluation subséquente devra tenir compte de cette valeur fixée arbitrairement.

5.3 Évaluer la sévérité de la perte des fonctions de sûreté des SIS.

L'évaluation de la sévérité a été réalisée par un « Chef de quart » de la centrale nucléaire à l'aide de la grille d'évaluation développée. Le tableau XIII présente les résultats de l'évaluation.

Tableau XIII : Résultats de l'évaluation de la sévérité

SIS	État de fonctionnement	Sévérité
RUC	Centrale en puissance	270
	Centrale à l'arrêt planifié	205
	PERCA +SDE 24 heures après	370
SEU	Centrale en puissance	105
	Centrale à l'arrêt planifié	105
	PERCA +SDE 24 heures après	330
ESR	Centrale en puissance	200
	Centrale à l'arrêt planifié	220
	Situation d'urgence	195
Caloporteur	Centrale en puissance	230
	Centrale à l'arrêt planifié	185
	Situation d'urgence	290
Modérateur	Centrale en puissance	325
	Centrale à l'arrêt planifié	365
	Situation d'urgence	405

5.4 Déterminer une valeur préliminaire pour les objectifs de fiabilité.

Les valeurs préliminaires ont été déterminées par un expert en fiabilité de la centrale nucléaire en tenant compte des informations pertinentes recueillies à l'étape 4.2. Le tableau XIV présente les valeurs qui ont été établies lors de cette phase.

Tableau XIV : Valeurs préliminaires

SIS	État de fonctionnement	Objectif de fiabilité
RUC	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-02
	PERCA +SDE 24 heures après	1E-02
SEU	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-03
	PERCA +SDE 24 heures après	1E-03
ESR	Centrale en puissance	1E-04
	Centrale à l'arrêt planifié	1E-04
	Situation d'urgence	1E-04
Grosse PERCA	Centrale en puissance	1E-02
	Centrale à l'arrêt planifié	1E-02
	Situation d'urgence	1E-02
Modérateur	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-03
	Situation d'urgence	1E-03

5.5 Évaluer la fréquence d'occurrence des défaillances majeures de procédé.

Selon la classification des SIS, il n'y a qu'un seul système de procédé dans le groupe à l'étude. Il s'agit du système caloporteur. L'objectif de fiabilité a été établi à 1E-02 et à de 1E-03 défaillance par année pour une petite perte de liquide caloporteur (PERCA) et pour la grosse PERCA. La somme de ces 2 défaillances est de 1,1E-02 défaillances par année. Le critère de défaillance « Simple » étant de 3E-01 défaillance majeure de procédé par année, les valeurs préliminaires fixées pour le système caloporteur sont acceptables.

5.6 Développer des séquences d'événements et les évaluer par rapport aux objectifs de sûreté

Compte tenu des ressources limitées, 6 événements initiateurs ont été évalués soit : la petite PERCA, grosse PERCA, « Design Basis Accident » (DBE), petite PERCA suivie d'un « Site Design Earthquake » (SDE) 24 heures après, grosse PERCA suivie d'un SDE 24 heures après et perte de SRR. Ces derniers ont été sélectionnés par un expert en fiabilité d'Hydro-Québec. Les séquences d'événement ont été développées en considérant la liste préliminaire de tous les SIS en vigueur lors de la rédaction de ce rapport. Les valeurs des autres SIS qui ne font pas partie du groupe sélectionné pour la validation sont préliminaires et n'ont pas été soumises à la validation finale. Seules les valeurs des systèmes à l'étude sont modifiées afin de respecter les objectifs de sûreté de la centrale. L'annexe G montre les séquences développées. Le tableau XV présente quant à lui les valeurs calculées pour chaque arbre d'événement en fonction de la probabilité de fonte du cœur et de relâche importante de matières radioactives à l'extérieur du B/R. Puisque la somme des probabilités pour tous les arbres d'événement est respectivement inférieure à 1E-04 et 1E-05 avec une certaine marge. Les objectifs de fiabilité permettent de répondre aux objectifs de sûreté. Toutes les branches menant à la relâche importante de matières radioactives à l'extérieur du confinement sont inférieures à une probabilité de 10E-07 relâche par année. Les scénarios sélectionnés ont été évalués lorsque la centrale est initialement en puissance seulement. Ils ne tiennent pas compte des scénarios lorsque la centrale est à l'arrêt planifié.

Tableau XV : Résultats des arbres d'événement

Scénarios	Probabilité de fonte du cœur (par an)	Probabilité de relâche importante (par an)
Petite PERCA (arrêt du réacteur)	1,00E-08	1,00E-08
Petite PERCA (boucle saine)	1,09E-07	1,09E-10
Petite PERCA (boucle rupturée)	1,91E-06	1,91E-09
Grosse PERCA (arrêt du réacteur)	1,00E-09	1,00E-09
Grosse PERCA (boucle saine)	1,09E-08	1,09E-11
Grosse PERCA (boucle rupturée)	1,01E-07	1,01E-10
Petite PERCA+ SDE (boucle saine)	2,83E-07	2,83E-10
Petite PERCA+SDE (boucle rupturée)	2,83E-07	2,83E-10
Grosse PERCA+SDE (boucle saine)	2,83E-08	2,83E-11
Grosse PERCA+SDE (boucle rupturée)	2,03E-08	2,03E-11
DBE (arrêt du réacteur)	2,19E-07	2,19E-07
DBE	2,74E-06	2,74E-09
SRR	1,00E-08	1,00E-08
Total:	5,73E-06	2,45E-07

5.7 Évaluer les arbres de défaillance des SIS de mitigation.

Dans le cadre de ce travail, des arbres de défaillance simplifiés ont été développés. Les arbres sélectionnés sont présentés à l'annexe H. Les valeurs préliminaires des systèmes de support ont été validées dans les arbres de défaillance des systèmes de mitigation tirés des arbres d'événement. Dans le groupe de SIS sélectionné, seul l'ESR constitue un système de support. Les arbres de défaillance du RUC et du modérateur permettent de valider l'objectif de fiabilité de l'ESR. Les valeurs des autres systèmes intégrés aux arbres de défaillance sont préliminaires puisque la validation à l'ensemble des SIS n'a pas encore été réalisée.

5.8 Compléter l'AMDEC des SIS et la valider la cohérence des valeurs préliminaires avec la matrice de risque.

L'annexe I présente les AMDEC des systèmes. La matrice du risque présentée au tableau XVI permet de montrer l'importance des systèmes en fonction du risque qu'ils présentent pour la centrale dans différents états de fonctionnement. La matrice démontre que les valeurs préliminaires sont cohérentes puisque les systèmes se situent tous dans les catégories de risque variant de « Moyen » à « Élevé ». Le RUC qui possède un objectif de fiabilité réglementaire est dans la catégorie « Élevé ». Les autres systèmes sont donc à un niveau acceptable.

Tableau XVI : Matrice de risque

Sévérité / Probabilité	Négligeable	Marginal	Important	Critique
Fréquent				
Probable	SEU (EN) SEU (AR)	RUC (AR)		
Occasionnel		Grosse PERCA (AR)		
Rare		ESR (EN) ESR (AR)	Grosse PERCA (UR)	
Improbable		ESR (UR)	SEU (UR)	RUC (UR)

5.9 Comparer avec les valeurs des autres centrales canadiennes.

Les valeurs établies par certaines autres centrales nucléaires canadiennes ont été recueillies et comparées aux valeurs préliminaires. Même s'il existe un certain écart, il a été déterminé par jugement d'expert de conserver les valeurs préliminaires puisque les données des autres centrales ne sont pas toutes disponibles et ne sont pas encore définitives. Des modifications pourront avoir lieu lorsque l'évaluation sera appliquée à

l'ensemble des SIS. Les valeurs des autres centrales ne sont pas présentées dans ce rapport puisqu'elles ne sont pas finales et qu'elles ne sont pas publiques.

À la lumière des nombreuses phases de validation, les objectifs de fiabilité pour le système sélectionné ont pu être déterminés. Ceci démontre que la méthodologie est cohérente et applicable à une centrale nucléaire de type CANDU 600 ne possédant pas d'ÉPS. Le tableau XVII présente les objectifs de fiabilité obtenus suite à son application.

Tableau XVII : Résultats de la validation

SIS	État de fonctionnement	Objectif de fiabilité
RUC*	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-02
	PERCA +SDE 24 heures après	1E-02
SEU*	Centrale en puissance	1E-02
	Centrale à l'arrêt planifié	1E-02
	PERCA +SDE 24 heures après	1E-02
ESR*	Centrale en puissance	1E-04
	Centrale à l'arrêt planifié	1E-04
	Situation d'urgence	1E-04
Grosse PERCA**	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-03
	Situation d'urgence	1E-03
Modérateur*	Centrale en puissance	1E-03
	Centrale à l'arrêt planifié	1E-03
	Situation d'urgence	1E-03

* Unités : année/année

**Unités : défaillance/année

CHAPITRE 6

CONCLUSION

La « Commission Canadienne de Sûreté Nucléaire » (CCSN) exige la mise en œuvre de la norme S-98 « Programme de fiabilité des centrales nucléaires ». Une des exigences de cette norme est d'établir les objectifs de fiabilité des SIS des centrales nucléaires canadiennes.

Une revue exhaustive de la littérature a permis de démontrer qu'il n'existait pas de méthodologie permettant de déterminer les objectifs de fiabilité des SIS. Cette dernière a été réalisée selon 3 critères de recherche soit le risque, la sûreté et les objectifs de fiabilité. Même si la revue de la littérature n'a pas permis de trouver une méthodologie applicable, elle a tout de même fait ressortir différents éléments pertinents à son développement.

Le but de ce projet était de développer une méthodologie permettant d'identifier, de classer et d'attribuer les objectifs de fiabilité des SIS d'une centrale nucléaire de type CANDU 600 dont l'évaluation probabiliste de sûreté ne repose pas sur l'ÉPS. Un des objectifs consistait à capturer une partie du savoir non-documenté provenant d'experts en accordant une attention particulière à l'approche de prise de décision conservatrice.

Une méthodologie a été développée de façon à tenir compte de tous les principes de sûreté et de toutes les exigences réglementaires pertinentes. Elle est inspirée de la nouvelle tendance dans l'industrie nucléaire qui consiste à prendre des décisions en utilisant la connaissance et la gestion du risque. La méthodologie est basée sur des techniques généralement reconnues. Il s'agit d'un processus où des valeurs préliminaires sont soumises à différentes phases de validation. Tout au long du processus, la cohérence des résultats est validée par le jugement d'experts.

La méthodologie développée est composée des 9 étapes suivantes:

1. Définir le concept d'objectif de fiabilité.
2. Recueillir les informations pertinentes concernant les SIS.
3. Évaluer la sévérité de la perte des fonctions de sûreté des SIS.
4. Déterminer une valeur préliminaire de l'objectif de fiabilité.
5. Évaluer la fréquence d'occurrence des défaillances majeures de procédé.
6. Développer des séquences d'événement et les évaluer par rapport aux objectifs de sûreté.
7. Évaluer les arbres de défaillance des SIS.
8. Compléter l'AMDEC des SIS, présenter leur criticité sur la matrice de risque et valider la cohérence des valeurs préliminaires.
9. Comparer avec les valeurs des autres centrales canadiennes.

Finalement, la méthodologie a été validée en l'appliquant à un groupe de SIS identifiés à la seule centrale nucléaire exploitée par Hydro-Québec. Cette phase a établi les objectifs de fiabilité de certains SIS représentatifs de toutes les classes de SIS identifiés à cette centrale. La validation a permis de déterminer que la méthodologie est cohérente et applicable à une centrale nucléaire de type CANDU 600 dont l'évaluation probabiliste de la sûreté ne repose pas sur l'ÉPS. À noter que les résultats présentés dans ce rapport ne sont pas nécessairement ceux qui seront établis lorsque la méthodologie sera appliquée de façon systématique à l'ensemble des SIS.

Tout au long de ce projet, une attention particulière a été apportée à la documentation des travaux. Ceci a répondu à l'objectif poursuivi qui consistait à capturer le savoir non documenté provenant d'experts en accordant une attention particulière à l'approche de prise de décision conservatrice. L'élaboration d'un questionnaire et l'évaluation de la criticité des SIS par un expert sont deux exemples qui ont contribué à capturer une partie des connaissances des experts ayant participé aux travaux.

Voici certaines recommandations qui font suite aux travaux réalisés dans le cadre de ce projet :

- Déterminer de façon détaillée les actions à prendre suite au dépassement des objectifs de fiabilité.
- Vérifier si la méthodologie peut être applicable à d'autres centrales que celles de type CANDU.
- Vérifier si l'établissement des objectifs de fiabilité est un sujet d'intérêt dans d'autres d'industries et voir si la méthodologie peut être applicable.
- Évaluer l'impact économique des objectifs de fiabilité.
- Réaliser une étude de sensibilité pour l'évaluation de la sévérité des systèmes à l'aide de la grille d'évaluation par différents experts.

RÉFÉRENCES BIBLIOGRAPHIQUES

1- Agence pour l'énergie nucléaire, (1993). *Assurer la Sûreté Nucléaire.* Organisation de coopération et de développement économiques, Paris

2- Agence pour l'énergie nucléaire, (2003), *L'énergie Nucléaire Aujourd'hui,* Organisation de coopération et de développement économique, Paris

3- Apostolakis, G.E., (2003), *How Useful is Quantitative Risk Assessment,* Massachusetts Institute of Technology, Engineering Systems Divisions, Boston.

4- Association canadienne de normalisation, (1998). *Overall Quality Assurance Program Requirements for Nuclear Power Plants,* CAN/CSA-N286.0-92, Rexdale, Ontario

5- Association canadienne de normalisation, (2002). *Gestion des risques : Guide à l'intention des décideurs.* (CAN/CSA-Q850-97). Etobicoke, Ontario

6- Beckjord, Eric. et al. (2003) *The Future of Nuclear Power.* Massachusetts Institute of Technology

7- Boyd, F.C. (1967) *Containment and siting requirements in Canada.* Proceedings of IAEA Symposium on the Containment and Siting of Nuclear Power Plants, Vienne. (AECL-2028)

8- Boyd, F.C., D.G. Hurst. (1972) *L'autorisation des réacteurs nucléaires, exigences de sécurité.* (CCEA-1059) Commission de contrôle de l'énergie atomique. Ottawa

9- Boyd, F.C. et al. (1964) *Pratique et expérience touchant la sécurité des réacteurs au Canada.* Présenté à la troisième conférence internationale des nations unies

sur l'utilisation de l'énergie atomique à des fins pacifiques. Session 3.6, p.318. Commission de contrôle de l'énergie atomique du Canada, Ottawa, Ontario. (AECL-2028-F)

10- Burford, G. et al. (1997). *Gestion des risques : Guide à l'intention des décideurs*, CAN/CSA-Q850-97, Association canadienne de normalisation.

11- COG, (2003) *Risk-significant Systems and Target Setting*, Working Group on Reliability Programs for CANDU Nuclear Power Plants, CNSC Workshop.

12- COG, (2006) *Risk-Informed Decision Making in the Canadian Nuclear Power Industry: Principles and Process*, CANDU Owners Group, Technical Working Group on Methods to Support Risk Informed Regulation. Rev-00

13- Commission canadienne de sûreté nucléaire, (2002), Regulatory Guide : Reliability program for Nuclear Power Plant. G-98, (Draft)

14- Commission canadienne de sûreté nucléaire (2005). *Principes fondamentaux de réglementation* (P-299). Ottawa

15- Commission canadienne de sûreté nucléaire (2005). *Études probabilistes de sûreté (ÉPS) pour les centrales nucléaires* (S-294). Ottawa.

16- Commission canadienne de sûreté nucléaire (2005*). Programmes de fiabilité pour les centrales nucléaires,* (S-98 révision 1). Ottawa.

17- Commission de contrôle de l'énergie atomique (C-006, rév. 1) Projet de guide de réglementation - *Analyse de sûreté des centrales nucléaires CANDU.* 1999

18- Department of Defense of United States Of America, (2000). *Standard Practice for System Safety*, MIL-STD-882D

19- Electric Power Research Institute, (1991). *Guidelines for the Safety Classification of Systems, Components, and Parts Used in Nuclear Power Plant Applications*, EPRI NP-6895,

20- Escobar L., Meeker, W. (2003). *Reliability: The other dimension of quality*, Louisiana state university; Iowa state university,

21- Golberg, B.E., et al. (1994) *System Engineering "Toolbox" for Design-Oriented Engineers*. (1358). NASA

22 HQ-802 (1999), *Advanced reactor safety design*. Hydro-Québec.

23- Hurst, D.G., F. C., Boyd. (1972), *Reactor licensing and safety requirements*, (AECB-1059). Commission de contrôle de l'énergie atomique.

24- IAEA-TECDOC-523 (1989). *Probabilistic safety criteria at the safety function/system level*. International Atomic Energy Agency.

25- IAEA (1999). *Basic Safety Principles for Nuclear Power Plants*. International Nuclear Safety Advisory Group. 75-INSAG-3 Rev.1, INSAG-12.

26- Lacroix, É. (1999). *Proposition d'une nouvelle structure d'évaluation probabiliste de sûreté pour les réacteurs CANDU PHW 600*, Université du Québec à Trois-Rivières.

27- Laurence, G.C. (1961) *Required Safety in Nuclear Reactors*. AECL-1923. Chalk River, Ontario

28- Laurence, G.C. (1962) *Operating Nuclear Reactors Safely*. Proceedings of Symposium on Reactor Safety and Hazards Evaluation Techniques 1, Vienne.

29- Marston, T. (1998) *The use of Level 3 PSA in the Risk-Informed, Performance-Based Regulation of Nuclear Power Plants.* (TR-109930) Newport Beach, California

30- Modarres, M. (1993). *What every engineer should know about reliability and risk analysis.* Marcel Dekker, New-York:

31- Modarres, M. et al. (2005). *A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen.* Reliability engineering and System Safety (89), pp. 271-285.

32- NEI 00-04 (Draft – Revision 0) (2003), *10 CFR 50.69 – SSC Categorization Guideline*, Nuclear Energy Institute. Washington DC.

33- New-Zealand/Australia Standards (2004). *Risk management* (AS/NZS 4360 :2004).

34- New-Zealand/Australia Standard (1998). *Risk analysis of technological systems-Application Guide* (AS/NZS 3931:1998).

35- Ordre des ingénieurs du Québec, *Formation intensive : Gestion des risques pour ingénieurs et autres spécialistes*, Université de Sherbrooke, 2005

36- Office Québécois de la langue française, *Le grand dictionnaire terminologique*, http://granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp, novembre 2005

37- Moore, P. (2005) *GSL Chair, Greenpeace Co-Founder, Attends UN Climate Change Conference : Says Nuclear « Part of Sustainable Future".* Canada NewsWire.

38- Petrilli, M-A. (2005). *Revue des pratiques internationales en matière de définition d'objectifs de sûreté fondés sur le risque*. Hydro-Québec.

39- Prince, P., et al. (2005), *L'énergie dans le monde : le passé et les avenirs possibles*, Canadian Energy Research Institute, Calgary, Alberta

40- Santamaura, P. (2002). *Generic CANDU Probabilistic Safety Assessment-Methodology*, (91-03660-AR-001 révision 0), Énergie Atomique du Canada Limitée.

41- Saqib, N., Siddiqi, M.T. (2005). *Threshold and goals for safety performance indicators for nuclear powers plant*. Reliability engineering and System Safety (87), pp. 275-286.

42- Siddall, E. (1954) *A study of serviceability and safety in the control system of the NRU reactor*. CRNE-582, Chalk River, Ontario

43- Siddall, E. (1959) *Statistical Analysis of Reactor Safety Standards*. Nucleonics. Vol. 17. No.2 , p. 64-69 (AECL-498)

44- Snell, V.G. (1978). *Sûreté des centrales nucléaires CANDU*. AECL-6329F

45- Snell, V.G., (2005) *Grouping and Separation*. CANDU Safety #9, CANTEACH

46- Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels*. Eyrolles. Paris, 795 p.

47- Zimmerman, T. (2003). *Reliability-Based Design and Assessment*, C-Fer Technologies.

ANNEXE A : GESTION ET PRISE DE DÉCISION UTILISANT LA CONNAISSANCE DU RISQUE

La sûreté des centrales nucléaires est assurée par la mise en œuvre de mesures permettant de réduire le risque à un niveau acceptable. La démarche entreprise concernant les objectifs de fiabilité des SIS s'inspire donc directement de la gestion du risque. Il a été jugé pertinent de décrire de façon détaillée ce concept puisque qu'il est à la base de toutes les activités entourant la sûreté des centrales nucléaires. De plus, la méthodologie développée pour déterminer les objectifs de fiabilité des SIS s'inspire de plusieurs éléments reliés à la gestion du risque. En plus de présenter ce processus, cette annexe décrit la nouvelle tendance dans l'industrie nucléaire qui consiste à la prise de décision en utilisant la connaissance et la gestion du risque. Cette annexe est principalement inspirée des références suivantes : 5, 6, 33, 34 et 35.

A.1 Gestion du risque

La gestion du risque peut être définie comme l'ensemble des activités mises en œuvre dans le but de le réduire à un niveau jugé acceptable. Elle peut être appliquée partout où une situation ou un événement non-désiré se produit ou encore lorsqu'une opportunité d'affaires se présente. Il s'agit d'un processus itératif composé de plusieurs étapes. Une réalisation adéquate de ces phases permet une amélioration continue du processus de prise de décisions. En général, la gestion du risque est reconnue comme partie intégrante d'une bonne pratique de gestion [6, 34]. Elle doit être incluse au niveau de la culture des entreprises. En effet, elle doit être intégrée dans la philosophie, la pratique et le plan d'affaires parce que les décideurs ont besoin de connaître toutes les conséquences possibles pour ainsi prendre les meilleures décisions. La figure A.1 présente le processus de gestion du risque.

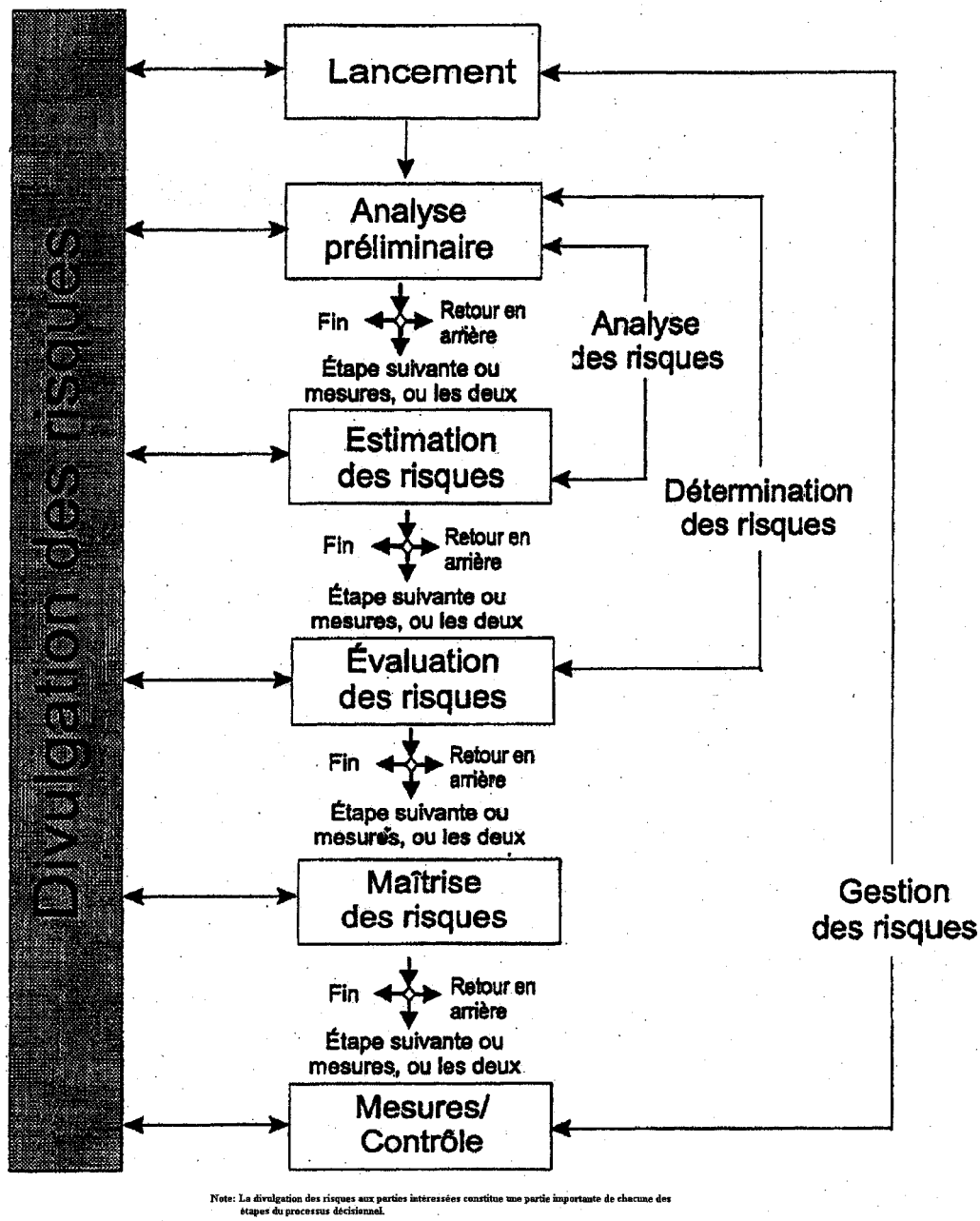


Figure A.1 Gestion des risques, étapes du processus décisionnel, modèle simple [5]

Voici quelques champs d'application de la gestion du risque [34] :

- Planification des ressources et la gestion des actifs;
- Changements : organisationnels, technologiques, politiques;
- Garanties sur les produits et services;
- Études de faisabilité;
- Investissements;
- Santé et sécurité au travail;
- Production et maintenance, et;
- Finances.

Le recours au processus de gestion du risque peut procurer des avantages considérables :

- Il offre une méthode complète et systématique d'analyse des problèmes qui aide à cerner la totalité des aspects du risque.
- Il intègre dans le processus décisionnel des perceptions des parties intéressées à l'égard de l'acceptabilité du risque. Ainsi, les décisions sont éclairées et les intérêts légitimes de l'ensemble des parties intéressées sont pris en compte.
- L'utilisation d'un processus décisionnel documenté et transparent permet aux décideurs de disposer d'arguments solides en faveur des décisions prises. Elle facilite l'explication des décisions et encourage le décideur à analyser le motif des décisions.
- L'utilisation d'un processus complet de gestion des risques peut entraîner des économies considérables de temps et d'argent.

Voici une description des différentes étapes du processus de gestion du risque :

A.1.1 Début du processus :

Une fois les risques cernés, une équipe de gestion du risque est formée. Voici les sous-étapes qui composent l'étape du lancement [5] :

- Détermination du problème;
- Formation d'une équipe de gestion du risque ;
- Attribution des responsabilités, du pouvoir et des ressources;
- Recensement des parties intéressées potentielles;
- Communication des considérations;
- Décisions, et;
- Exigences de documentation.

A.1.2 Appréciation du risque

L'une des étapes les plus complexes est celle de l'appréciation du risque. Elle permet d'évaluer le risque en fonction des conséquences et de leur probabilité d'occurrence et de les comparer avec le risque défini comme acceptable. Elle est composée des sous étapes suivantes :

a. Analyse du risque;
    - Déterminer la probabilité d'occurrence (fréquence) de l'événement non-désiré;
    - Déterminer les conséquences (gravité) de l'événement non-désiré;
b. Estimation du niveau du risque;

c. Évaluation du risque, et;

d. Acceptation du risque.

L'analyse du risque peut être définie comme l'utilisation systématique de renseignements permettant de cerner les dangers et d'estimer la probabilité et la gravité d'effets sur les personnes ou les populations (blessures ou pertes), les bien matériels, l'environnement et autres valeurs. Il existe un certain nombre de méthodes normalement utilisées dans les analyses liées à la gestion du risque. Quelques-unes de ces méthodes ont été présentées lors de la revue de la littérature. La sélection d'une méthode dépend du but de l'analyse, de la complexité du système analysé, du niveau de risque, des compétences du personnel impliqué, etc.

L'estimation du risque est un processus visant à estimer la fréquence ou la probabilité et les conséquences de certains scénarios de risque en considérant l'incertitude des estimations. Les résultats de l'estimation du risque peuvent être présentés sous forme de matrices de risque (fréquence-gravité). La figure A.2 présente un exemple de ce genre de matrices.

Fréquence de l'occurrence	**Gravité**			
	Catastrophique	**Majeure**	**Mineure**	**Négligeable**
Fréquente	A	A	A	C
Probable	A	A	B	C
Occasionnelle	A	B	B	D
Faible	A	B	C	D
Improbable	B	C	C	D

Figure A.2 : Matrice du niveau de risque (fréquence-gravité) [5]

L'évaluation du risque est un processus consistant à examiner les risques sur le plan des coûts et des avantages et à effectuer une évaluation de l'acceptabilité des risques en considérant les besoins, les intérêts et les préoccupations des parties intéressées.

Le résultat d'une telle démarche est la détermination de l'acceptabilité des risques. En fait, l'absence de risque est peu fréquente sauf dans le cas où l'activité à l'origine du risque est abandonnée [5]. Plutôt que de s'efforcer à supprimer totalement les risques, il est préférable d'essayer de les réduire à un niveau aussi bas qu'il est raisonnablement possible d'atteindre. Ce principe porte le nom d'ALARA/ALARP [5] ; La figure A.3 illustre ce concept.

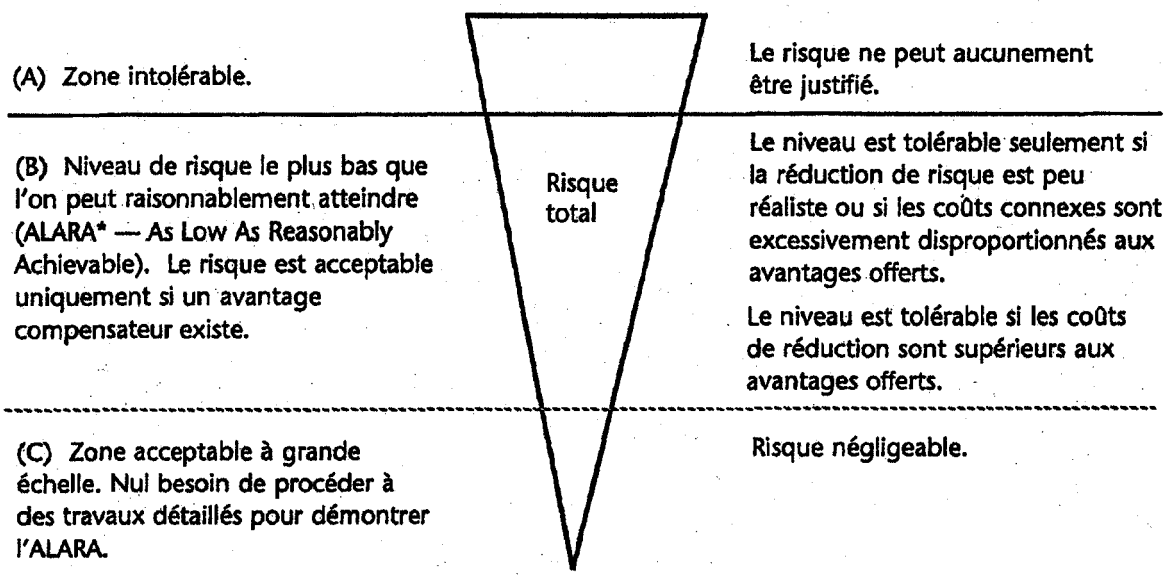


Figure A.3 : ALARA/ALARP – Cadre d'établissement des critères relatifs aux risques [5]

Plusieurs facteurs ont une influence sur l'acceptation du risque par les parties intéressées. Leur perception est issue des besoins, des intérêts et des préoccupations exprimés par les parties intéressées. Elle a donc une influence sur les décisions s'articulant autour de l'acceptabilité du risque [5]. Les facteurs qui peuvent changer la

perception du risque peuvent être d'ordre éthique, moral, économique, politique, etc. Quels que soient les critères d'acceptation, il est indispensable qu'ils soient connus et explicités à toutes les phases d'analyse. La meilleure façon de déterminer le niveau de risque acceptable est d'assurer un dialogue efficace entre les parties intéressées [5].

A.1.3 Maîtrise du risque

La maîtrise du risque désigne l'ensemble des actions ou des dispositions entreprises en vue de diminuer la probabilité ou la gravité des dommages associés à un risque particulier. De telles mesures doivent être envisagées lorsque le risque est jugé inacceptable. Elles doivent être considérées et mises en œuvre tant et aussi longtemps que le risque n'est pas au niveau souhaité. Pour évaluer leur efficacité, il convient d'estimer le risque avant et après l'application des mesures. Les coûts, les avantages, le risque résiduel et les risques associés aux mesures de maîtrise doivent être pris en considération au moment de l'évaluation.

Dans certains cas, les mesures pour contrôler et mitiger les risques sont simples et évidentes. Elles peuvent impliquer des modifications pour se conformer aux pratiques standards. Dans d'autres cas, des mesures alternatives doivent être envisagées afin de trouver la meilleure solution. Il est important de considérer plusieurs possibilités. Par exemple, la modification des installations physiques n'est pas toujours la méthode la plus appropriée pour contrôler et mitiger les risques.

La maîtrise du risque peut être réalisée par l'une des approches suivantes [34] :

- Éviter le risque en décidant de ne pas réaliser l'activité qui peut le générer;
- Réduire la probabilité d'occurrence;
- Réduire les conséquences;

- Transférer le risque, ou;
- Retenir le risque.

La priorité des mesures de maîtrise du risque devrait toujours être accordée à celles qui permettent d'éliminer le danger ou encore d'en réduire la probabilité d'occurrence. Les mesures de maîtrise du risque devraient être utilisées selon l'ordre suivant :

- Prévention;
- Détection;
- Contrôle;
- Mitigation, et;
- Mesures d'urgence.

Avant de choisir les stratégies de maîtrise du risque, il convient de les soumettre aux parties intéressées. Une mesure proposée peut sembler acceptable pour le décideur au niveau de l'efficacité et du coût mais être inacceptable pour d'autres parties intéressées en raison d'autres facteurs. Il importe d'évaluer toute mesure proposée ou toute stratégie de financement sous l'angle des besoins, des intérêts et des préoccupations des parties intéressées.

A.1.4 Divulgation des risques, communication et consultation

La divulgation des risques consiste en une communication entre les parties intéressées au sujet de l'existence, de la nature, de la forme, de la gravité et de l'acceptabilité d'un risque.

Une communication efficace est importante pour s'assurer que les personnes responsables de la mise en œuvre du processus de gestion du risque et celles y ayant un intérêt comprennent la base sur laquelle les décisions sont prises et pourquoi certaines actions sont requises.

La communication et la consultation impliquent un dialogue constant entre les parties intéressées. L'effort doit être concentré plutôt sur la consultation et le dialogue. En effet, puisque les parties intéressées peuvent avoir un impact significatif dans la prise de décision, il est important que leurs préoccupations soient identifiées et documentées.

A.1.5 Mesures et contrôle

Cette étape consiste à mettre en œuvre les stratégies de maîtrise du risque, à évaluer l'efficacité du processus décisionnel et à établir le programme de contrôle. Cette étape est composée des sous-étapes suivantes [5] :

- Élaboration d'un plan de mise en œuvre
- Mise en œuvre des stratégies de maîtrise, de financement et de communication
- Établissement d'un processus de contrôle :
    - Contrôle des changements;
    - Contrôle de la performance;
    - Mise en œuvre appropriée des stratégies de maîtrise, de financement et de communication;
    - Contrôle de l'exactitude des hypothèses, et;
    - Calendrier d'exécution.
- Évaluation de l'efficacité du processus décisionnel axé sur la gestion des risques

A.1.6 Documentation

Chaque étape du processus de gestion du risque doit être documentée. La documentation doit inclure les éléments suivants [5]:

- Détails de l'ensemble des évaluations des mesures réalisables de maîtrise des risques et de financement des risques;
- Détails de l'ensemble des hypothèses servant aux analyses;
- Description des données et des méthodes servant à l'analyse des mesures de maîtrise et de financement;
- Description des incertitudes liées aux résultats des analyses;
- Obligation des tiers à l'égard de la mise en œuvre des stratégies de maîtrise et de financement;
- Copies de la totalité des contrats relatifs aux stratégies de maîtrise et de financement;
- Considération des parties intéressées relativement aux stratégies proposées de maîtrise et de financement, et;
- Motifs de l'ensemble des décisions;

Les raisons suivantes justifient l'élaboration de la documentation :

- Démontrer que le processus est réalisé correctement.
- Fournir la preuve que les étapes d'identification et d'analyse des risques sont réalisées d'une manière systématique.
- Fournir les enregistrements sur les risques et développer une banque de données concernant le savoir et le savoir-faire quant aux risques de l'entreprise.

- Fournir aux décideurs un plan de gestion des risques pour l'approbation et la mise en œuvre.
- Fournir un outil et un mécanisme de suivi et de comptabilité.
- Fournir les informations nécessaires pour la conduite des audits.
- Divulguer les informations pertinentes.

A.2 Prise de décision utilisant la connaissance et la gestion du risque

Le concept de prise de décision utilisant la connaissance et la gestion des risques est relativement récent dans l'industrie nucléaire. Le terme utilisé en anglais est « *Risk Informed Decision Making* ». Il comprend l'intégration des éléments probabilistes, déterministes et non quantifiables de telle manière que la prise de décision est réalisée en tenant compte du risque dans son ensemble. Les résultats d'une évaluation probabiliste ne devraient pas constituer le seul intrant à la prise de décision [3]. Ce processus se base principalement sur la gestion du risque présentée précédemment.

Voici les principes fondamentaux de cette philosophie [12] :

- Elle est utilisée dans l'évaluation de problèmes ayant un impact potentiel sur la sûreté ou sur l'aspect réglementaire. L'utilisation efficace et efficiente des ressources est proportionnelle au niveau de risque généré par le problème analysé.
- Elle utilise toutes les informations à la disposition des preneurs de décision. Ceci inclut les évaluations déterministes et probabilistes, le jugement qualitatif d'ingénieur basé sur l'expérience, l'état de la centrale et d'autres facteurs intangibles difficilement quantifiables.
- L'objectif des calculs probabilistes est de présenter les données quantitatives qui contribuent à la prise de décision en tenant compte des solutions proposées ou

de l'orientation de l'action à prendre. Ces calculs ne doivent pas être vus comme les seuls intrants à la prise de décision.

- L'évaluation adoptée sera fonction de la nature et de la portée du problème. Elle sera cohérente avec le but de l'évaluation en question. Elle sera réalisée de manière à s'assurer que les méthodes déterministes et probabilistes sont intégrées et qu'elles incorporent un niveau de conservatisme réaliste.
- Les critères de jugement considérés dans la prise de décision seront appliqués de manière à :
  - Intégrer les analyses déterministes et celles basées sur le risque;
  - Maintenir l'intégrité de la défense en profondeur;
  - Assurer une marge de sûreté suffisante;
  - Prendre en considération les objectifs de sûreté appropriés, et;
  - Considérer le cadre réglementaire dans lequel la décision doit être prise.
- Le principe de défense en profondeur est incorporé dans la prise de décision de façon à déterminer les mesures compensatoires nécessaires. Il est important de souligner que la défense en profondeur est une stratégie permettant d'assurer la protection du public lorsqu'une incertitude non quantifiable est présente dans l'évaluation du risque.

ANNEXE B : PRINCIPES DE SÛRETÉ DES CENTRALES NUCLÉAIRES

Les principes à la base de la sûreté des centrales nucléaires représentent l'ensemble des mesures spécifiques inspirées du principe de gestion des risques que s'est dotée l'industrie nucléaire pour assurer la sûreté de ses installations. En fait, ces principes permettent d'atteindre les objectifs de sûreté de façon à répondre au risque défini comme acceptable. Ils peuvent être répartis en 5 catégories : objectifs généraux de sûreté, les principes reliés à la gestion, la stratégie de défense en profondeur, les principes techniques généraux et les principes spécifiques [25]. Cette annexe présente ces fondements ainsi qu'une description de certaines particularités de sûreté des centrales nucléaires de type CANDU 600. Elle permet de comprendre de quelle façon est appliquée le concept de gestion du risque pour assurer la sûreté des centrales nucléaires. Cette annexe est inspirée des documents suivants : 1, 2, 25, 44 et 45.

B.1 Objectifs généraux de sûreté

L'industrie nucléaire s'est dotée d'objectifs généraux de sûreté qui permettent de s'assurer que les installations présentent un risque négligeable pour la population. En fait, trois objectifs généraux de sûreté sont poursuivis par les centrales nucléaires soit l'objectif général de sûreté, l'objectif en radioprotection et l'objectif technique de sûreté [25].

L'objectif général de sûreté stipule qu'il faut protéger les individus, la société et l'environnement en établissant et en préservant une défense efficace contre les risques radiologiques provenant des centrales nucléaires. L'objectif premier de sûreté des centrales est d'éviter la dispersion de radioactivité vers l'environnement et la population [1].

L'objectif de radioprotection a pour but d'assurer qu'en exploitation normale, l'exposition aux radiations à l'intérieur et à l'extérieur de la centrale soit aussi basse que possible.

Ceci est réalisé en tenant compte des facteurs sociaux, économiques, des limites prescrites et en assurant la limitation de l'exposition aux radiations suite à un accident.

L'objectif technique consiste à prévenir les accidents nucléaires et ce, avec un grand niveau de confiance. De plus, il s'agit de s'assurer que tous les accidents considérés dans la conception auraient des conséquences minimes et que la probabilité d'occurrence d'accidents ayant des conséquences radiologiques majeures soit extrêmement faible.

B.2 Principes reliés à la gestion

Une culture de sûreté qui soutient les actions de tous les individus et de toutes les organisations impliqués de près ou de loin dans une activité reliée à l'industrie nucléaire doit absolument être mise en place. Un des éléments d'une culture de sûreté consiste en une politique de sûreté dans laquelle sont énoncés les objectifs et les engagements des organisations concernant la protection du public. Les gestionnaires doivent instaurer des pratiques et des attitudes qui favorisent cette culture. La sûreté est la responsabilité de tous les travailleurs. Elle est atteinte lorsque ceux-ci adoptent une attitude interrogative, une approche rigoureuse et prudente ainsi qu'une communication adéquate. La responsabilité ultime pour la sûreté des centrales nucléaires revient à l'exploitant. Cependant, il ne faut toutefois pas négliger la responsabilité des concepteurs, des fournisseurs, des entrepreneurs, des constructeurs et des législateurs.

Chaque gouvernement doit établir une législation entourant l'industrie nucléaire. En fait, chaque état doit former une organisation responsable d'accorder les permis d'exploitation, de contrôler les centrales nucléaires et de modifier les règlements. Elle doit être entièrement indépendante de façon à ce qu'en aucun cas, elle puisse être influencée dans ses décisions. Elle doit avoir comme mission principale d'assurer la protection de la population [25]. Au Canada, c'est la CCSN qui joue ce rôle.

B.3 La défense en profondeur

Le principe de défense en profondeur est l'élément clé de la sûreté des centrales nucléaires [22]. Il est basé sur l'hypothèse que les systèmes et les êtres humains ne sont pas parfaits et que par conséquent des défaillances peuvent avoir lieu [44]. La conception des centrales doit être en mesure de compenser pour ces défaillances. La défense en profondeur consiste à fournir plusieurs niveaux de protection qui ont pour but d'empêcher la relâche importante de matières radioactives à l'environnement. Ils sont mis en place de façon à protéger les différentes barrières afin d'éviter qu'elles ne soient endommagées par un accident et qu'elles ne puissent compenser pour une erreur humaine ou encore une défaillance mécanique potentielles. Cette philosophie assure que la sûreté ne dépend pas seulement d'un élément dans la conception, la construction, la maintenance ou l'opération d'une centrale nucléaire. Le principe de défense en profondeur est divisé en cinq niveaux de protection [2]. La figure B.1 présente le principe de défense en profondeur.

Une emphase particulière est mise sur le premier niveau qui consiste à s'assurer que la probabilité qu'un système ou qu'un composant défaille soit minime [25]. Ceci dans le but de prévenir un accident potentiel. Il peut être atteint par des standards de qualité élevés, une conception conservatrice, des bonnes pratiques d'exploitation, une assurance qualité adéquate pour être certain que les exigences de conception sont respectées, une surveillance efficace permettant de détecter les dégradations, des procédures mises en place pour éviter qu'une défaillance ne puisse se développer en un accident majeur, etc. En plus d'augmenter le niveau de sûreté, ces mesures contribuent également à maximiser la productivité des installations [1].

La détection et la maîtrise des défaillances constituent le deuxième niveau de protection de la défense en profondeur. Il est essentiel de pouvoir détecter rapidement les déviations par rapport au fonctionnement normal de façon à ce qu'elles soient maîtrisées efficacement. Dans une situation idéale, l'écart devrait être automatiquement

corrigé par les systèmes de contrôle et de protection sans perturber le fonctionnement normal.

La troisième ligne de défense est la maîtrise des accidents de dimensionnement. Dans l'éventualité où un événement anormal rend les systèmes de contrôle et de protection défaillants, des systèmes de sauvegarde, conçus pour être fiables et efficaces, permettent d'amener automatiquement la centrale dans un état stable et de confiner les matières radioactives. La conception de ces systèmes est réalisée pour qu'ils puissent résister aux accidents inclus dans l'enveloppe de dimensionnement. Ils ont comme fonction de s'assurer que les matières radioactives soient constamment confinées, que le réacteur soit arrêté très rapidement et que la chaleur résiduelle soit évacuée après l'arrêt pour préserver l'intégrité des barrières permettant d'éviter la dispersion de la radioactivité. La première barrière de protection est la matrice des pastilles et la gaine de protection du combustible qui retiennent la plus grande partie des produits radioactifs. Dans le cas où les gaines de combustible seraient endommagées, le circuit caloporteur, qui est un circuit fermé, permet de retenir les produits de fission. Finalement, le confinement constitue la dernière barrière de protection permettant de prévenir le rejet important de matières radioactives à l'extérieur de l'enceinte du bâtiment réacteur. Le confinement est prévu pour résister à la pire rupture d'une conduite du circuit primaire.

Le quatrième niveau de protection a pour but d'atténuer les conséquences d'un accident sévère et de prévenir une dispersion importante de la radioactivité à l'extérieur du confinement. Le cinquième niveau consiste à réduire les conséquences radiologiques sur la population dans le cas d'une relâche importante de matières radioactives grâce à la mise en œuvre d'un plan d'urgence. Par exemple, un plan d'évacuation doit être établi ou encore des mesures doivent être entreprises pour éviter que les matières radioactives ne soient transmises via la chaîne alimentaire suite à un accident nucléaire.

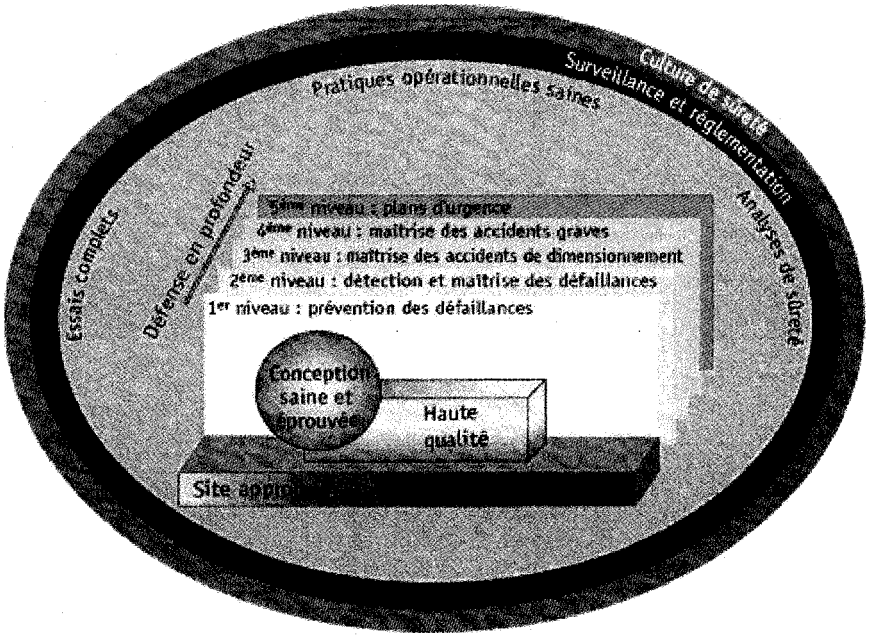


Figure B.1 : Les 5 niveaux de protection de la défense en profondeur. [2]

B.4 Principes techniques généraux

Il existe plusieurs principes techniques qui permettent à une centrale nucléaire d'atteindre ses objectifs de sûreté.

Tout d'abord, la technologie utilisée dans les centrales nucléaires doit s'inspirer de pratiques reconnues et doit respecter les codes et les standards internationaux. Dans cet esprit, le recours à des fournisseurs approuvés augmente le niveau de confiance. De plus, la standardisation peut indirectement procurer un niveau de sûreté plus élevé puisque les fournisseurs concentreront leurs efforts sur un nombre restreint d'équipements. Cependant, il faut faire attention car la diversité de conception est un élément important permettant de prévenir les défaillances de cause commune. L'évolution dans la conception des équipements standardisés permet de réduire le risque de problèmes génériques [25].

L'assurance qualité doit être appliquée à toutes les activités d'une centrale nucléaire pour garantir que les tâches réalisées répondront aux exigences avec un grand niveau

de confiance. La qualité, la fiabilité des équipements ainsi que la performance humaine sont au cœur de la sûreté des centrales nucléaires. Il faut donc assurer la qualité par des contrôles et des vérifications documentés réalisés dans le cadre d'un programme établi. Ce dernier fournit la structure nécessaire pour l'analyse des tâches, le développement des méthodes, l'établissement des standards et l'identification des compétences et des équipements nécessaires [25].

Un autre principe technique de sûreté est l'auto évaluation. Il consiste en une évaluation de chaque activité importante par des individus à l'intérieur de l'organisation de façon à déterminer son efficacité et d'identifier les opportunités d'amélioration. Ce principe permet d'assurer l'implication du personnel en lien avec les objectifs organisationnels en détectant les problèmes de sûreté et en tentant de les résoudre. L'auto évaluation est un processus complémentaire à celui des audits d'assurance qualité et des revues de sûreté réalisés par du personnel indépendant.

L'évaluation par les pairs permet d'avoir accès aux pratiques et aux programmes utilisés par les meilleures centrales nucléaires dans le monde entier dans le but de les faire partager à l'ensemble de l'industrie nucléaire. Elle est réalisée par un groupe d'experts indépendants. Un exemple d'évaluation par les pairs est celle de la « World Association of Nuclear Operators » (WANO).

Pour la sûreté d'une centrale nucléaire, les facteurs humains sont très importants à considérer. En fait, le personnel impliqué dans des activités en lien avec la sûreté des centrales nucléaires doit être formé et qualifié pour le travail à accomplir. La conception de la centrale doit être réalisée de façon à faciliter la prise de décision par l'opérateur. De plus, elle doit permettre de détecter, compenser ou corriger les erreurs humaines. Ce facteur est très important puisque dans le passé, plusieurs incidents mineurs se sont transformés en accidents majeurs à cause d'erreurs de nature humaine [25]. Il est primordial de considérer l'action de l'opérateur lors du déroulement de l'incident. Les séquences d'événement développées doivent donc absolument tenir compte de ce facteur.

L'évaluation de la sûreté est réalisée avant la construction et l'exploitation d'une centrale nucléaire. Elle est documentée et révisée de façon indépendante. De plus, elle doit être à jour de façon à refléter l'évolution de la centrale en fonction des différentes modifications. L'évaluation est réalisée pour s'assurer que la centrale répond aux objectifs de sûreté fixés. Tel que présenté auparavant, il existe principalement deux méthodes permettant de répondre à cet objectif soit l'analyse de type déterministe et celle de type probabiliste.

En ce qui a trait à la radioprotection, des pratiques doivent être mises en œuvre de façon à respecter les recommandations de l'«International Commission on Radiological Protection» (ICRP) et de l'AIEA pour toutes les phases du cycle de vie d'une centrale nucléaire. Ces mesures sont prises pour protéger les travailleurs et le public contre les effets nocifs des radiations.

L'expérience d'exploitation et les résultats de recherche concernant la sûreté doivent être communiqués, révisés et analysés. Les organisations doivent apprendre des situations anormales et doivent adopter des mesures appropriées afin d'éviter que ces événements ne se reproduisent.

Finalement, le dernier principe technique est l'excellence en exploitation. Elle est atteinte en augmentant la culture de sûreté, la défense en profondeur, en améliorant la performance humaine, en assurant le bon fonctionnement des équipements par un bon programme de maintenance préventive et prédictive, en pratiquant l'auto évaluation et l'évaluation par les pairs, en échangeant l'expérience en exploitation et d'autres informations avec des partenaires dans le monde entier, en augmentant l'utilisation de l'ÉPS et en élargissant la mise en œuvre de la gestion des accidents sévères [25]. L'amélioration de la performance humaine nécessite une attention particulière puisque plusieurs événements majeurs y sont attribuables.

L'adoption de ces principes fondamentaux ne garantit pas à une centrale nucléaire l'élimination complète du risque. Cependant, ils permettent certainement de le réduire à un niveau acceptable et constituent une base essentielle dans l'atteinte des objectifs de sûreté. De nos jours, l'excellence en exploitation est souvent reliée à l'augmentation de la disponibilité des centrales et à la diminution des coûts [25]. Cependant, ces gains ne doivent en aucun cas réduire le niveau global de sûreté des centrales nucléaires et ils doivent s'inscrire dans la volonté de l'industrie nucléaire de maintenir la sûreté des installations.

B.5 Sûreté des CANDU

Puisque la méthodologie permettant de déterminer les objectifs de fiabilité des SIS est principalement développée pour une centrale nucléaire de type CANDU, les éléments de sûreté intégrés à la conception de ce type de centrale sont présentés. Cette section facilite la compréhension de la gestion des incidents et des hypothèses de base émises pour l'évaluation de la sûreté des CANDU. Elle est divisée en 3 parties : le regroupement et la séparation, les systèmes spéciaux de sûreté et les considérations de sûreté des CANDU.

B.5.1 Le regroupement et la séparation:

Le regroupement et la séparation ont pour but d'offrir une protection contre un événement qui affecte une partie de la centrale. Ils permettent d'éviter que des défaillances de cause commune entraînent la perte d'une des fonctions de sûreté. En pratique, ils assurent que les interconnections entre les systèmes ne viennent pas modifier leur efficacité suite à un accident.

Le regroupement consiste à s'assurer qu'il existe au moins deux façons indépendantes d'accomplir chaque fonction principale de sûreté. Le regroupement consiste à séparer les systèmes reliés à la sûreté (SRS) en 2 groupes. Ces regroupements ont été réalisés de façon à ce que chaque groupe puisse réaliser indépendamment toutes les fonctions de sûreté. Dans cette optique, les deux systèmes d'arrêt d'urgence sont séparés pour

éviter qu'un événement ne puisse empêcher l'arrêt du réacteur. De plus, le RUC et le confinement sont aussi dans des groupes distincts pour empêcher qu'un seul accident ne puisse à la fois endommager le combustible et entraîner la relâche de matières radioactives à l'extérieur du B/R. Le tableau B.I présente les différents SRS en fonction de leur groupe et de leurs fonctions de sûreté.

Tableau B.I : Répartition des SRS selon les 2 groupes et leur fonction de sûreté [45]

Fonctions de sûreté	Groupe 1	Groupe 2
Arrêt du réacteur	- Système de régulation du réacteur - SAU#1	- SAU#2
Refroidissement du combustible	- Système caloporteur - RUC - RTA - Modérateur - GV et circuit secondaire	- Système d'eau d'urgence (SEU)
Confinement	- Climatisation du B/R	- Confinement
Surveillance et contrôle	- Salle de commande principale	- Salle de commande d'urgence
Support aux systèmes	- Catégorie IV - Catégorie III (diesels) - Catégorie II - Catégorie I	- Alimentation électrique d'urgence (AEU) - Catégorie II - Catégorie I
	- Eau de service re-circulée - Eau brute de refroidissement	- Système d'eau d'urgence
	- Système d'air d'instrumentation	- Réserves d'air locales

En plus du regroupement, les CANDU sont conçus de façon à ce qu'il y ait une séparation physique entre les systèmes. Les groupes situés à l'extérieur du bâtiment réacteur sont séparés de 90 degrés. Par exemple, l'AEU et le SEU sont situés dans des bâtiments différents. Les systèmes du groupe 2 sont généralement qualifiés sismiques. De plus, ils doivent être situés au-dessus du niveau potentiel d'inondation d'un bâtiment. La salle de commande principale est protégée des conséquences de certains événements. Cependant, une seconde salle de commande distante de la première a été conçue pour résister à un événement sismique majeur et permettre d'opérer les fonctions importantes du réacteur. Un chemin d'accès qualifié sismique reliant la salle

de commande principale à celle d'urgence a été conçu de façon à ce que les opérateurs puissent accéder à la salle de commande d'urgence si une situation l'exige.

À l'intérieur du réacteur, des barrières ou une séparation physique sont appliquées autant que faire ce peut. Lorsque la séparation physique ne peut être mise en œuvre certains principes doivent être appliqués :

- Il doit être démontré qu'il n'y a pas d'accidents susceptibles de se produire dans cette zone.
- Un autre système du groupe 2 permettra d'atténuer les conséquences.
- Le système ou ses composants sont séparés par des barrières.
- Le système ou ses composants sont sûrs après la défaillance (« Fail Safe »).
- Les composants résistent à l'accident.

Au niveau de l'instrumentation, une logique 2 de 3 a été instaurée de façon à diminuer le nombre d'arrêts intempestifs et de permettre de réaliser des essais en marche, les 3 signaux pouvant être comparés entre eux. Ceci permet à l'opérateur de détecter une situation anormale.

Voici d'autres principes de conception des CANDU concernant la séparation à l'intérieur d'un même groupe [45] :

- L'alimentation électrique des composants redondants à l'intérieur d'un groupe est divisée en alimentations paire et impaire.
- Il existe des séparateurs pour les connections entre la salle de commande principale et la salle de commande d'urgence.
- Les dispositifs permettant de contrôler la réactivité du réacteur sont situés à l'extérieur du système caloporteur sous pression pour éviter qu'ils soient éjectés ou encore détériorés par une hausse de pression du caloporteur.

De façon générale, la conception des CANDU a été réalisée de façon à ce qu'il y ait deux groupes séparés pour lesquels le principe de redondance est appliqué. Les besoins de qualification des équipements sont déterminés par rapport à leur fonction de sûreté. Il doit y avoir le moins de connections possibles entre les deux groupes pour éviter les défaillances de cause commune. La diversité de conception est un autre élément très important pour la sûreté des centrales nucléaires [45]. Tous ces dispositifs et principes de conception sont mis en œuvre afin de prévenir les défaillances de cause commune qui pourraient entraîner la perte d'une fonction de sûreté et ainsi provoquer un incident majeur. Ils s'inscrivent dans le processus de gestion du risque.

B.5.2 Les Systèmes Spéciaux de Sûreté (SSS)

La conception des SSS a été réalisée de façon à ce qu'ils puissent minimiser les conséquences du pire scénario d'accident. Ce dernier a été déterminé comme étant le bris complet d'un collecteur d'entrée du système caloporteur (grosse PERCA). Une telle défaillance aurait pour effets d'augmenter la pression à l'intérieur du confinement, la réactivité et la température des gaines de protection du combustible.

La conception des systèmes d'arrêt d'urgence du réacteur a été réalisée en considérant ce scénario combiné à une indisponibilité du confinement. Ils devaient être en mesure de limiter l'augmentation de la réactivité de façon à ce que la chaleur puisse être évacuée par le RUC et la portion restante du caloporteur. Ces exigences ont été formulées dans le but d'éviter la dégradation des gaines de protection du combustible due à une augmentation importante de la température ainsi qu'une relâche importante de matières radioactives à l'extérieur du B/R. Au début, les CANDU ne possédaient qu'un seul système d'arrêt d'urgence. Cependant, l'analyse de la défaillance d'un système de procédés qui aurait pour effet d'augmenter la réactivité combinée à la défaillance du système d'arrêt d'urgence réalisée pour évaluer la capacité du confinement comportait trop d'incertitudes. Il a été décidé d'intégrer un deuxième système d'arrêt complètement indépendant permettant de prévenir un accident

nucléaire majeur. Il a été décidé de séparer les systèmes d'arrêt d'urgence des systèmes de régulation du réacteur.

Les systèmes d'arrêt d'urgence et le RUC doivent agir conjointement pour éviter la dégradation du combustible lors d'une grosse PERCA. Pour ce faire, le RUC a été doté d'une logique qui permet de connaître l'endroit du bris de façon à envoyer l'eau au collecteur du côté opposé. Le réacteur est situé au point le plus bas du système caloporteur ce qui assure qu'il sera inondé par l'eau du RUC. Dans le cas où le RUC s'avérerait indisponible, le modérateur pourrait servir comme source froide ultime de relève.

Finalement, le confinement est doté de certains dispositifs lui permettant d'assurer l'étanchéité du B/R et de participer à la suppression d'énergie de façon à préserver son intégrité et de diminuer le taux de fuite.

B.5.3 Autres considérations de sûreté des CANDU

Les centrales CANDU utilisent l'uranium (UO_2) naturel comme combustible et l'eau lourde comme modérateur. Cette combinaison procure certains avantages au niveau de la sûreté. Tout d'abord, l'UO_2 ne peut atteindre la criticité que dans l'eau lourde. Par exemple, les grappes de combustible usées peuvent être entreposées dans des piscines d'eau légère sans danger qu'une réaction en chaîne ne survienne. Un autre avantage important de la conception des CANDU est que l'arrangement géométrique du combustible à l'intérieur du réacteur est réalisé de façon à procurer une réactivité optimale. Donc, si une distorsion ou une dispersion du combustible survient, il n'y aura pas d'augmentation de la réactivité. Dans le cas d'un bris de gaine, l'uranium naturel ne réagirait pas chimiquement avec l'eau chaude. L'UO_2 possède une conductivité thermique moins élevée que les combustibles à base de métaux et de carbone. Ceci ralentit les réactions divergentes lors de phases de transition. Cette réponse plus lente est un avantage certain au niveau des systèmes de contrôle et de sûreté. Finalement, le combustible possède une température de fusion relativement élevée.

ANNEXE C : ÉVALUATION DE LA SÛRETÉ DES CENTRALES NUCLÉAIRES

L'établissement des objectifs de fiabilité est directement influencé par la façon dont est réalisée l'évaluation de la sûreté d'une centrale nucléaire. Pour que la méthodologie développée soit applicable, il faut absolument tenir compte des techniques utilisées pour évaluer le niveau de sûreté de la centrale nucléaire. Cette annexe présente les principales approches utilisées pour réaliser cette évaluation. Elle fournit un historique de l'évaluation de la sûreté au Canada et aux États-Unis qui permettra de bien comprendre l'évolution de l'évaluation de la sûreté des centrales nucléaires au cours des années et de situer la démarche entreprise par la CCSN. Finalement, les hypothèses de base émises lors de l'évaluation de la sûreté des centrales nucléaires sont présentées.

C.1 Approche déterministe de sûreté

L'approche déterministe, comme son nom l'indique, constitue une analyse des phénomènes physiques susceptibles de survenir dans un état de système donné. Les analyses de sûreté de type déterministe sont réalisées pour démontrer que les systèmes de la centrale, en particulier les SSS, sont conçus et exploités de façon à respecter les exigences. Elles permettent de s'assurer que les conséquences des accidents graves de procédé faisant partie de l'enveloppe de dimensionnement respectent les limites prescrites [22]. En pratique, une série d'événements initiateurs susceptibles de provoquer un accident pouvant constituer un risque inacceptable sont déterminés. Ensuite, une analyse technique est réalisée afin de prévoir la réponse de la centrale et de celle des systèmes de sûreté impliqués sans tenir compte de la probabilité d'occurrence des événements. Ainsi, il est possible d'évaluer le niveau de risque pour chaque scénario et de s'assurer qu'il demeure à l'intérieur des limites réglementaires. Les études déterministes n'analysent que les 30 premières minutes suivant l'incident. Cette approche a mené au concept de défense en profondeur des installations nucléaires [22].

Les analyses déterministes se basent sur les critères de défaillances « Simple/Double » (« Single/Dual Failure »). EACL s'est basé sur le principe suivant pour développer cette approche : la dose résultant d'une défaillance ayant une forte probabilité d'occurrence (défaillance simple) doit être inférieure à la dose provenant d'une séquence d'événements moins probable de survenir (défaillance double) [22]. À partir de ce principe, deux critères ont été établis. Tout d'abord, il ne doit pas y avoir plus d'une défaillance majeure de procédé par 3 ans (défaillance simple). Cette probabilité a été établie pour que la dose absorbée par le public en général soit égale à la dose limite permise par la loi pour une année. L'autre critère stipule que la probabilité qu'une défaillance majeure de procédé soit combinée à une défaillance d'un SSS (Défaillance double) doit être inférieure à 1 par 3 000 réacteurs-ans. Cette dose limite de référence a été jugée tolérable pour une dose d'urgence dans une vie. Il fixe donc l'objectif de fiabilité des SSS à 1E-03 année/année. Il a été estimé que l'exposition à cette dose pourrait entraîner une augmentation de 0,1% des risques de cancer dans une population de 1 million d'habitants. Le tableau C.I présente les doses limites.

Tableau C.I : Doses limites de référence en condition normale et anormale [8].

Situation	**Fréquence maximale**	**Conditions atmosphériques à considérer**	**Dose maximale individuelle**	**Dose totale maximale à la population**
Opération normale	100%	Pondérées selon l'effet	0.5 rem/an (tout le corps)	10^4 homme-rem
Défaillance majeure de procédé	1/3 ans	Pondérées selon l'effet	3 rem/an à la thyroïde	10^4 thyroïde rem/an
Défaillance majeure de procédé plus défaillance d'un système de sécurité	1/3000 ans	Pire condition atmosphérique qui survient 10% du temps ou condition de Pasquill F	25 rem/an (tout le corps) 250 rem à la thyroïde	10^6 homme-rem 10^6 thyroïde-rem

Malgré le fait que cette approche définit précisément les exigences d'efficacité pour les SSS, elle comporte certains inconvénients majeurs :

- Ne permet pas de cibler la variation importante des taux d'occurrence et des conséquences des différents scénarios à l'étude.
- Ne permet pas de bien traiter les défaillances des systèmes de support qui peuvent entraîner à la fois la défaillance d'un SSS et d'un système de procédés.
- Ne permet pas d'exprimer efficacement le besoin en disponibilité des SSS après un accident.
- Ne cible pas le besoin de tenir compte des modes communs de défaillance à l'étape de la conception qui pourraient entraîner la défaillance des 2 groupes de systèmes.

C.2 Approche probabiliste de sûreté

L'évaluation probabiliste permet d'évaluer la probabilité d'occurrence d'un événement et de ses conséquences. Elle sert à estimer le risque et à repérer les faiblesses potentielles. Elle a permis de déterminer que certains systèmes ayant été établis comme critiques par l'analyse déterministe de sûreté sont considérés comme non-critiques et vice-versa. Malgré le fait que l'approche probabiliste a permis d'identifier certains maillons faibles, la sûreté d'une centrale nucléaire est principalement évaluée en fonction des analyses déterministes. Celles de type probabiliste viennent donc les compléter. L'étude de fiabilité, l'étude matricielle de sûreté et l'étude probabiliste de sûreté sont trois techniques utilisées pour réaliser l'évaluation probabiliste de la sûreté.

C.2.1 Étude matricielle de sûreté (ÉMS)

Pour palier aux lacunes de l'approche de défaillances « Simple/Double », les concepteurs d'EACL ont proposé en 1975 une technique d'analyse appelée « Étude Matricielle de Sûreté » (ÉMS) [22]. Contrairement à la technique précédente, ces

analyses tiennent compte des interdépendances entre les systèmes, des actions effectuées par l'opérateur et de l'opération suite à un accident. Les études matricielles de sûreté consistent en une évaluation probabiliste de sûreté qui analyse les scénarios possibles suite à une série d'événements initiateurs déterminés. Elles déterminent la réponse de la centrale suite à leur avènement. Elles commencent par un événement initiateur. Un arbre événementiel est ensuite réalisé jusqu'à ce que les séquences critiques atteignent une probabilité inférieure à 10E-07 ou jusqu'à l'atteinte d'un état stable [14]. Les ÉMS présentent les interactions critiques entre les systèmes. Leur conception facilite la compréhension du fonctionnement de la centrale en condition anormale et l'évaluation des actions de l'opérateur. Elles permettent de déterminer la criticité des différents systèmes de la centrale et déterminent les activités humaines ainsi que les procédures nécessaires pour éviter que les conséquences mènent à un accident nucléaire majeur. Les arbres de défaillances et les arbres d'événements sont deux outils permettant l'élaboration des matrices de sûreté.

Les avantages de l'ÉMS sont [26] :

- Analyse quantitative et qualitative qui offre une bonne compréhension des causes et des conséquences des événements initiateurs.
- L'analyse d'un seul accident par étude permet de bien comprendre la réponse de la centrale face à cette situation en particulier.
- Les réponses développées sont fonction des différentes causes de l'événement initiateur.
- Les causes et leur importance sont clairement identifiées.
- Le niveau de détail des études est très élevé.
- Permet de créer une liste d'hypothèses et d'activités d'exploitation créditées dans le modèle.
- Les études sont de moins grandes envergures et sont plus faciles à modifier.
- Considère le déroulement de la réponse dans le temps.

- La représentation graphique des séquences d'événement facilite la compréhension.
- Meilleure compréhension de la réponse de la centrale et des interactions dans une condition anormale d'exploitation.
- Identification des actions requises par l'opérateur dans une condition anormale d'exploitation.
- Identification des modifications de conception désirables.
- Identification des besoins de conception telles que la redondance et la séparation des systèmes reliés à la sûreté.

Les inconvénients de l'ÉMS sont [26] :

- Ne fournit pas une vision globale de la sûreté de la centrale puisque chaque événement est traité de façon indépendante.
- Les erreurs d'exploitation ne sont pas considérées.
- L'étude matricielle sur le confinement n'est pas aussi détaillée qu'une ÉPS de niveau 2.
- Il n'existe pas de normes concernant les ÉMS.
- La méthode est unique aux centrales de type CANDU.

C.2.2 Étude probabiliste de sûreté (ÉPS)

Une étude probabiliste de sûreté est une technique analytique qui permet d'intégrer différents aspects de conception et d'opération de façon à évaluer la sûreté d'une installation [40]. L'ÉPS représente la nouvelle orientation internationale en terme d'évaluation de sûreté. En effet, cette technique a maintenant remplacé les études matricielles de sûreté dans certaines centrales nucléaires canadiennes et est largement répandue dans les autres pays [15, 26, 40]. Elle est généralement utilisée pour déterminer la fréquence d'occurrence de la fonte du cœur et la fréquence de relâche importante de substances radioactives à l'extérieur du confinement afin d'avoir une idée de la sûreté globale de la centrale. La correspondance entre la conception et

l'exploitation est évaluée en identifiant des événements initiateurs qui présentent un risque important et en désignant les composants qui contribuent le plus au scénario d'accident. Les arbres de défaillances et les arbres d'événements sont les deux principaux outils permettant l'élaboration des ÉPS. Les ÉPS peuvent être de trois niveaux différents en fonction des objectifs poursuivis :

Niveau 1- Analyse des systèmes.

Une ÉPS de niveau 1 détermine et quantifie les séquences d'évènement conduisant à une perte de l'intégrité structurelle du cœur et à des défaillances massives de combustible.

Niveau 2- Analyse des systèmes et du confinement.

En plus de l'analyse de niveau 1, elle analyse le comportement du confinement, évalue les radionucléides émis par le combustible défaillant et quantifie les rejets dans l'environnement.

Niveau 3- Analyse des conséquences.

En plus de celle de niveau 2, elle analyse la distribution des radionucléides dans l'environnement et évalue le risque pour la santé publique ainsi que les conséquences économiques de l'accident.

L'ÉPS de niveau 3 intègre les incertitudes des trois niveaux [29]. Il existe des techniques pour traiter ces incertitudes et les résultats obtenus par une ÉPS de niveau 3 peuvent donner une idée du risque que présente une centrale nucléaire pour la population [29]. Cependant, les ÉPS de niveau 3 sont moins pratiquées à cause des efforts qu'elles demandent et de la précision des résultats.

EACL suggère une méthodologie pour mettre en oeuvre une ÉPS qui comporte 12 étapes [40] :

1- Collecte de l'information
2- Analyse des événements initiateurs
3- Développement des arbres d'événement
4- Analyse de la fiabilité du système
5- Analyse des défaillances de cause commune
6- Analyse de la fiabilité humaine
7- Développement d'une base de données
8- Quantification des séquences d'événement
9- Analyse des états de dommage pour la centrale
10- Analyse d'incertitude et de sensibilité
11- Assurance qualité
12- Diffusion des résultats

Voici les principales contributions de l'ÉPS [26] :

- Permet de vérifier que la conception est complète et cohérente
- Évalue les modifications apportées à la conception
- Évalue les stratégies de gestion et d'exploitation
- Permet d'optimiser les stratégies d'entretien, d'essai et de formation
- Aide à se prononcer sur l'opportunité de réaliser des interventions pour amélioration
- Évalue les stratégies de réponse aux accidents
- Assure un contrôle systématique du niveau de sûreté
- Établit les priorités pour la recherche future
- Aide à créer de nouveaux concepts de réacteurs

Voici les limites de l'ÉPS [26] :

- Dépendante de la conception déterministe
- Incertitudes dans les données et les modèles
- Demande des ressources importantes
- Difficulté d'analyse de certains problèmes
- Conclusions sélectives de l'équipe qui réalise l'ÉPS

C.2.3 Étude de fiabilité

Les études de fiabilité évaluent la probabilité et la fréquence de défaillance des systèmes et de leurs composants [26]. Elles servent à démonter la fiabilité des SSS et des SRS crédités dans les ÉMS.

Les principaux objectifs d'une étude de fiabilité sont de :

- Fournir un portrait de l'état réel d'exploitation du système;
- Évaluer les caractéristiques de fiabilité du système;
- Déterminer les composants critiques qui contribuent fortement à l'indisponibilité et à la défaillance;
- Identifier les tâches requises pour minimiser l'indisponibilité du système, et;
- Déterminer les règles d'exploitation lors de certaines défaillances partielles.

Une étude de fiabilité est composée de plusieurs éléments. Elle comprend une description du système et de ses composants, une identification des principales hypothèses et des données de fiabilité utilisées. Ensuite, les résultats sont présentés et une analyse de sensibilité est réalisée. En général, l'étude de fiabilité est basée sur la technique des arbres de défaillance.

C.3 Historique de l'évaluation de la sûreté aux États-Unis

Comme la majorité des développements dans le domaine de l'énergie nucléaire, les premières préoccupations en terme de sûreté ont débuté avec le projet « Manhattan » pendant la deuxième guerre mondiale [31]. Dans les années 1940, les ingénieurs de la compagnie « Du Pont » ont amené les concepts d'indépendance structurelle et fonctionnelle qui ont contribué au développement du principe de défense en profondeur. Dans le but de contourner les incertitudes de l'époque, les ingénieurs de l'« Atomic Energy Commission » (AEC), organisme responsable de la réglementation nucléaire à l'époque, ont proposé d'utiliser l'approche déterministe basée sur des hypothèses et des calculs conservateurs. Les experts de l'AEC ont défini une série d'accidents de référence. Ces derniers devaient représenter les pires scénarios envisageables dans une centrale nucléaire. La réponse de la centrale était alors évaluée en fonction de ces accidents de référence. Cette approche était fondée sur l'hypothèse suivante : si la centrale peut contrer les accidents de référence, elle est en mesure de répondre adéquatement à tous les autres accidents.

Le rapport « WASH-740 » considérait la grosse PERCA comme la cause la plus importante de dangers de relâche importante de matières radioactives à l'environnement [31]. En considérant cet événement, les analyses ont permis de déterminer que le confinement ne pouvait plus être considéré comme une barrière complètement étanche à la radioactivité.

Au début des années 1970, la population américaine exprimait un besoin grandissant de connaître le niveau de sûreté des centrales nucléaires. En 1972, l'AEC a désigné Norman Rasmussen, professeur au département nucléaire du «Massachusetts Institute of Technology » (MIT), pour réaliser une étude portant sur la sûreté des centrales nucléaires nommée « Reactor Safety Study » (RSS). L'équipe formée pour cette étude était composée d'environ 40 scientifiques et ingénieurs provenant de différents domaines. Au début, seuls les arbres de défaillance étaient utilisés pour calculer le

risque des réacteurs. Cependant, l'équipe s'est rendu compte que l'intégration de toutes les analyses dans un seul arbre de défaillance pour toute une centrale était trop complexe. Ceci a mené au développement des arbres d'événement qui furent utilisés pour évaluer la réponse de la centrale. Contrairement à la tendance dans ce temps, l'équipe a étudié à partir des arbres d'événement plusieurs déviations possibles. Elle n'analysait pas seulement la grosse PERCA comme événement initiateur.

Les résultats ont été présentés dans un rapport connu sous le nom de « WASH-1400 ». Parmi les principales conclusions, il a été démontré que la petite PERCA possédait la plus grande contribution au risque tandis qu'elle était négligée auparavant. De plus, il a été statué qu'un accident impliquant la fonte du cœur aurait des conséquences modestes pour la population. Le rapport affirmait aussi que la probabilité de défaillance du confinement était plus grande que celle envisagée.

Le rapport fut l'objet de nombreuses controverses. Le sommaire était au cœur des discussions puisqu'il affirmait que le risque présenté par 100 réacteurs nucléaires était beaucoup moins grand que plusieurs autres activités humaines comme l'automobile, l'avion, etc.

Suite à cette controverse, un comité dirigé par le Dr Harold Lewis a été mandaté pour faire la révision du RSS. Le comité de révision a noté plusieurs qualités au rapport dont l'utilisation des arbres de défaillances et des arbres d'événement. Cependant, il a apporté plusieurs critiques dont la plus importante concernait l'utilisation faite du rapport par certaines instances. En 1978, le NRC a retiré le rapport « WASH-1400 » et a fait modifier tous les documents qui y faisaient référence.

En mars 1979 est survenu l'accident de Three Miles Island. Cet incident a permis de démontrer qu'un incident relativement mineur a mené à une PERCA. De plus, le rôle de

l'opérateur a été démontré comme un facteur très important comme le suggérait le rapport de Rasmussen. Suite à ces démonstrations, le NRC a rétabli le RSS.

L'accident de Three Miles Island et le rapport « Lewis » ont permis de déterminer qu'il était dorénavant nécessaire d'utiliser l'évaluation probabiliste de sûreté pour compléter les analyses déterministes. Ceci a mené au développement d'une technique qui correspond à la nouvelle orientation internationale soit l'ÉPS. Malgré l'émergence de l'évaluation probabiliste de sûreté, le NRC a clairement statué que le principe de défense en profondeur constituait toujours un élément essentiel pour assurer la sûreté des centrales nucléaires [31]. À l'heure actuelle, la prise de décision en utilisant la connaissance du risque prend de plus en plus d'importance dans le processus d'évaluation de sûreté.

C.4 Historique de l'évaluation de la sûreté au Canada

Le développement de la philosophie canadienne en terme d'évaluation de sûreté des centrales nucléaires a fortement été influencé par un accident survenu dans un réacteur expérimental en 1952 [22]. Cet incident a permis de constater que malgré une bonne conception et une bonne construction, les systèmes sont défaillants. L'accident a démontré que des mesures de sécurité plus simples et un bon entretien permettraient d'offrir une meilleure protection que des équipements compliqués à maintenir en état. À partir de ce moment, il était nécessaire d'avoir des systèmes de sûreté indépendants pouvant être testés régulièrement de façon à faire la preuve qu'ils sont disponibles pour accomplir leur mission. Le concept de défense en profondeur est un des éléments clés de la philosophie de sûreté canadienne [22].

En 1954, une étude ayant pour but de prédire la performance opérationnelle d'un nouveau réacteur, le NRU, a été réalisée [42]. Cette analyse a permis d'instaurer le principe de la logique « 2 de 3 » qui consiste à tripler les circuits de contrôle du réacteur de façon à réduire le nombre d'arrêts intempestifs dus à la défaillance d'un circuit tout en augmentant la sécurité des systèmes. Cette nouvelle conception a aussi permis de

tester les circuits sans avoir à arrêter le réacteur. À l'époque, cette étude présentait le plus grand avancement au niveau du contrôle des réacteurs depuis l'accident du NRX [42].

En 1959, une première étude tentant d'évaluer le risque provenant des réacteurs nucléaires en le comparant avec celui d'autres industries a été réalisée [43]. Elle utilisait la valeur monétaire de production par vie perdue comme base statistique de comparaison. Selon l'étude, les centrales nucléaires devaient être 5 fois plus sécuritaires que celles au charbon. Certains critères ont été établis à partir de cette hypothèse de base. Tout d'abord, il ne devait pas y avoir plus de 1 défaut du système caloporteur par 50 ans. De plus, il ne devait pas y avoir plus d'une défaillance totale d'un système de sûreté par 500 occasions en considérant que le caloporteur et le système de régulation du réacteur sont défaillants. Cette valeur pouvait être diminuée à 1 par 50 ans pour une défaillance partielle du système. Finalement, le système de régulation du réacteur ne devait pas être défaillant plus de 1 fois par 160 ans lorsque le réacteur est à pleine puissance et que la réactivité est croissante.

Une autre étude est arrivée à des conclusions similaires en 1961 [44]. Elle avait comme hypothèse qu'une relâche importante de matières radioactives devait avoir une fréquence d'occurrence de moins de 10E-05 par année pour un taux de mortalité de 10E-02 par réacteur-an [44]. Ce niveau de risque avait été fixé de façon à être moins élevé que les autres types d'industries tout en étant atteignable. Les objectifs ont été établis en divisant les systèmes selon 3 catégories en tenant compte de la difficulté d'estimation des défaillances de cause commune ainsi que des défaillances sur les pièces non dupliquées. Tout d'abord, les systèmes de procédé ne devaient pas être défaillants plus de 1 fois par 10 ans. De plus, il devait y avoir moins de 1 défaillance par 100 (10E-02) demandes pour les systèmes de sûreté et pour le confinement. La combinaison de la défaillance de ces trois types de systèmes (défaillance triple) qui entraînerait une relâche importante de matières radioactives avait donc un objectif cumulé de 10E-5 par année.

Ces objectifs ont été réajustés un an plus tard à 0,3 défaillance par an pour les systèmes de procédés et 3X10E-03 pour l'indisponibilité des systèmes de sûreté et du confinement [28].

En 1964, les limites de la zone d'exclusion ont été fixées de façon à ce qu'une personne située à l'extérieure des frontières ne reçoivent pas des doses supérieures à 25 rem pour le corps entier et 250 rads à la thyroïde sauf pour quelques conditions atmosphériques extrêmement rares suite à une défaillance d'un système de procédés combinée à celle d'un système de sûreté (défaillance double) [9].

En 1967, des doses limites ont été ajoutées pour considérer la défaillance d'un système de procédé (défaillance simple) [44]. Ces dernières ont été présentées au tableau C.I. Ces doses sont calculées en tenant compte des pires conditions atmosphériques survenant 10% du temps.

En 1972, EACL a établi une série de critères concernant les exigences de sûreté pour l'autorisation des réacteurs nucléaires au Canada dans un document de référence communément appelé le « Siting Guide » [8]. À partir de cette époque, le confinement n'a plus été considéré comme une simple unité mais plutôt comme un assemblage de sous-unités [23]. De plus, les systèmes d'arrêt, le système de refroidissement d'urgence du cœur (RUC) et le confinement ont été regroupés comme étant des Systèmes Spéciaux de Sûreté (SSS). Les SSS doivent être indépendants entre eux et indépendants des systèmes de procédé. L'approche d'évaluation de sûreté des centrales nucléaires proposée dans le « Siting Guide » est celle des défaillances « Simple/Double ». Lors de la conception des CANDU, toutes les défaillances des systèmes de procédé ont été analysées de façon à s'assurer qu'ils respectaient les exigences de défaillance simple. En ce qui a trait aux systèmes de contrôle, seule la pire défaillance a été analysée en supposant que si la protection était adéquate contre cet événement, elle le serait pour tous les autres. Ensuite, toutes les défaillances simples ont été analysées en les combinant avec la défaillance de chacun des SSS de façon à démontrer que les limites prescrites par la défaillance double étaient respectées.

Il semble y avoir un nombre invraisemblable de combinaisons à réaliser mais ce n'est pas le cas. Par exemple, lors d'une perte de contrôle de la puissance du réacteur, le caloporteur est toujours disponible et il n'est pas nécessaire de considérer cette défaillance avec celle du RUC.

Au fil des ans, les réacteurs étaient devenus plus gros et possédaient des inventaires plus grands de produits de fission. De plus, un plus grand nombre d'événements étaient considérés dans la matrice des défaillances doubles. L'indisponibilité des systèmes de sûreté a par conséquent été réduite à 10E-03 et la fréquence de défaillance d'un système de procédé de 1 par 3 ans a été interprétée comme étant la défaillance totale de tous les systèmes de procédés. Ces exigences plus restrictives reflètent davantage le besoin d'assurer la sûreté d'un nombre grandissant de réacteurs que d'un réacteur en particulier.

Afin de palier aux lacunes de l'approche de défaillances « Simple/Double », les ingénieurs d'EACL ont développé en 1975 une technique analytique nommée « Étude matricielle de sûreté» (ÉMS). À cette époque, elle constituait un avancement important en terme d'évaluation de la sûreté des centrales nucléaires [22]. Cependant, elles ne procurent aucune information quant au niveau global de sûreté de la centrale nucléaire puisque que les séquences d'événement ne sont pas reliées entre elles. Dorénavant, certaines centrales nucléaires canadiennes utilisent l'ÉPS pour évaluer leur sûreté. Il est à noter que contrairement aux autres centrales dans le monde, les centrales nucléaires canadiennes n'ont pas senti le besoin immédiat d'adopter l'ÉPS puisqu'elles possédaient déjà un outil permettant de tenir compte des actions de l'opérateur. Cette nécessité avait été adressée suite à l'accident de Three Miles Island [22]. La CCSN songe à exiger l'utilisation de l'ÉPS pour évaluer la sûreté des centrales nucléaires au Canada [15].

C.5 Hypothèses de base

Certaines hypothèses ont été formulées lors de la conception des CANDU et de la réalisation des analyses de sûreté. Elles définissent collectivement l'enveloppe d'exploitation sécuritaire [22]. Voici certaines des hypothèses jugées pertinentes :

- Lors d'un accident, la défaillance d'arrêt du réacteur est considérée comme non-crédible. Cette hypothèse fait en sorte d'éviter d'analyser de nombreux scénarios d'accident avec le réacteur en puissance où l'incertitude des résultats est significative. Les rapports de sûreté et les ÉMS ne font aucune analyse des scénarios avec le réacteur non-arrêté. La raison qui permet d'émettre cette hypothèse est la présence de deux systèmes d'arrêt d'urgence indépendants dans les réacteurs CANDU [22]. En tenant compte de cet aspect, les deux systèmes d'arrêt d'urgence ont une importance particulière.
- L'action d'opérateur est créditée dans les scénarios d'accident. Pour que son action puisse être créditée, certaines conditions doivent être remplies. En fait, la formation de l'opérateur est adéquate, les salles de commande doivent être habitables, il reçoit les indications nécessaires et l'opérateur est capable d'exécuter l'action spécifique nécessaire. Il a été jugé que les salles de commande principale et d'urgence (habitabilité et opérabilité) ainsi que leurs équipements ont une importance particulière pour la sûreté de la centrale.
- Certains systèmes servent de relève aux SIS. L'importance de ces systèmes ne peut être démontrée par une analyse uniquement quantitative (exemple : modérateur comme source froide de relève du RUC).
- Les systèmes pouvant initier ainsi que ceux servant à prévenir un accident ont une importance particulière. Il est crucial de minimiser l'occurrence des événements initiateurs et celle d'utilisation des systèmes de mitigation suite à un incident (prévention des accidents).

ANNEXE D : GRILLE D'ÉVALUATION

Une grille a été élaborée afin de faciliter l'évaluation de la sévérité des SIS par un expert. Elle est constituée d'une série d'énoncés jugés pertinents pour évaluer l'importance du rôle joué par chacun des systèmes pour la sûreté de la centrale nucléaire. Cette annexe présente une explication de chacun des énoncés qui constituent la grille. Voici la description de chacun de ces critères d'évaluation.

1- Quel est le délai de repli suite à la perte de la fonction de sûreté?

Cet élément a été intégré en se basant sur l'hypothèse que plus le délai accordé à l'exploitant pour prendre action est court, plus la perte de la fonction de sûreté est critique. Par exemple, une perte de fonction de sûreté nécessitant une action immédiate est plus critique qu'une qui requiert qu'une action soit posée au prochain arrêt. Les délais sont généraux et permettent à l'expert d'exercer son jugement.

2- Quelle est l'action de repli suite à la perte de la fonction de sûreté?

De la même façon que l'énoncé précédent, il a été supposé que plus l'action de repli nécessaire est significative, plus la perte de la fonction de sûreté est importante. En effet, un événement qui nécessite le déclenchement d'un système d'arrêt d'urgence est nécessairement plus sévère qu'un incident pour lequel l'état de fonctionnement normal peut être conservé.

3- Quel est l'état de repli suite à la perte de la fonction de sûreté?

L'état dans lequel doit être mise la centrale suite à la perte de la fonction de sûreté a aussi été considéré comme un élément permettant de déterminer la sévérité de la perte d'une fonction de sûreté.

4- Quelle est la fonction de sûreté?

Il existe une hiérarchisation au niveau des fonctions de sûreté assurées par l'opérateur pour stabiliser l'état de la centrale suite à un événement. Il est donc important de tenir compte de cet élément lors de l'évaluation de la sévérité de la perte de la fonction de sûreté.

5- La perte de la FS est susceptible de causer la défaillance d'autres SIS ?

Cet énoncé permet d'évaluer les défaillances de cause commune. Si la défaillance d'un système entraîne la défaillance d'autres SIS, elle est susceptible de causer un événement majeur. Il est donc essentiel d'accorder une importance particulière à ce facteur. De plus, cet énoncé permet de mettre l'emphase sur les systèmes de support. La défaillance d'un SIS réduisant l'accessibilité des opérateurs à d'autres SIS est un facteur considéré pour évaluer ce critère.

6- La perte de la FS est susceptible de causer la défaillance de SRS ?

Cet énoncé a été ajouté puisqu'il a été jugé pertinent de considérer les défaillances de cause commune pour les SRS qui ne sont pas SIS. En fait, cette nuance est importante puisqu'un système entraînant la défaillance de plusieurs systèmes même s'ils ne sont pas SIS est susceptible de provoquer un incident majeur qui sera plus difficile à gérer pour l'opérateur. Par exemple, la défaillance d'un SIS réduisant l'accessibilité des opérateurs à d'autres SRS est un facteur considéré pour évaluer ce critère.

7- Il existe d'autres systèmes qui permettent de compenser la perte de la FS ?

Il est évident que si un système constitue la dernière barrière de protection suite à un événement, il est significativement plus critique pour la sûreté qu'un autre

système pour lequel la perte de la fonction de sûreté peut être compensée de plusieurs autres façons. Cet énoncé évalue le niveau de redondance de la fonction de sûreté.

8- La perte de la FS entraîne la perte d'une ou plusieurs barrières de la défense en profondeur ?

Tel que présenté précédemment, le concept de défense en profondeur est à la base de la conception des centrales nucléaires et permet d'assurer la protection du public. La défaillance d'un système qui entraîne la perte d'une des barrières de la défense en profondeur est considérée comme importante au niveau de la sûreté.

9- Est-ce qu'une procédure permet à l'opérateur d'atténuer facilement les conséquences de la perte de la FS?

Si l'opérateur possède une procédure claire, validée, pour laquelle il possède un niveau élevé de confiance et qui est relativement facile à mettre en pratique, il sera en mesure d'atténuer efficacement la défaillance d'un système. Une perte de fonction de sûreté assurée par un SIS qui est bien couverte par une procédure peut être considérée moins critique qu'une autre pour laquelle l'opérateur ne possède pas de document en support à sa décision ou encore que sa formation ne lui a pas permis d'être confronté à la situation.

10- Est-ce que la perte de la FS réduit la capacité de l'opérateur à prendre des décisions permettant d'atténuer les conséquences de l'événement ?

Cet énoncé a été élaboré de façon à considérer les défaillances qui entraînent une perte de la fonction surveillance qui réduit l'information nécessaire à l'opérateur pour prendre une décision éclairée. Il considère le niveau de stress

de l'opérateur lors d'une situation donnée car il est reconnu que ce facteur influence fortement le niveau de performance humaine.

11- La perte de la FS est susceptible d'entraîner des doses aux travailleurs, et/ou à l'environnement et au public ?

Puisque la sûreté des centrales nucléaires a pour but de d'empêcher les doses aux travailleurs, à l'environnement et au public qui pourraient entraîner une dégradation de la vie, il est essentiel de considérer l'importance d'une perte de fonction de sûreté par rapport aux doses susceptibles d'être émises.

ANNEXE E : SYSTÈMES IMPORTANTS POUR LA SÛRETÉ

La validation de la méthodologie développée est réalisée sur un groupe de SIS d'une centrale nucléaire exploitée par Hydro-Québec. Puisque la méthodologie est appliquée de façon différente aux groupes de SIS, il s'avère nécessaire de présenter les grandes familles de SIS identifiées dans cette installation. À noter que l'identification des SIS de cette centrale n'est pas encore finalisée. Certains des systèmes présentés dans ce rapport pourront être enlevés de cette liste et d'autres systèmes pourront y être ajoutés. La méthodologie utilisée pour procéder à l'identification des SIS, les classes de SIS ainsi qu'une brève description de chaque système du groupe sélectionné sont présentées dans cette annexe. Cette dernière permettra donc de mieux comprendre comment la méthodologie développée sera appliquée en fonction du rôle joué par chacun de ces systèmes.

E.1 Méthodologie pour l'identification des SIS de la centrale nucléaire

La méthodologie développée pour déterminer la liste des SRS et SIS est inspirée de documents de référence [4, 19, 32], des approches d'autres centrales ainsi que de travaux antérieurs réalisés à la centrale. La méthodologie a été établie pour permettre de passer systématiquement en revue tous les systèmes et de déterminer ceux qui sont importants pour la sûreté. Voici les principales étapes :

a) Trier une liste exhaustive des systèmes en centrale. La sélection consiste à déterminer les systèmes qui ne sont pas critiques pour la sûreté en utilisant la définition de la norme CAN/CSA-N286.0-92 pour les systèmes de A à G [4].

b) Trier les systèmes en se basant sur les fonctions de sûreté. Les systèmes sélectionnés doivent assurer l'une des 4 fonctions principales.

c) Sélectionner les systèmes qui permettent d'atténuer les accidents postulés et documentés dans certains rapports et certaines analyses d'Hydro-Québec. Les systèmes retenus à partir de cette étape sont classés dans la catégorie A/B/C/D selon la définition de la norme CAN/CSA-N286.0-92 [4] et/ou selon la priorité A/B/C définie ultérieurement dans un autre projet réalisé par Hydro-Québec.

d) Révision et validation de la liste préliminaire des SIS et des SNCS (systèmes non critiques pour la sûreté) par le groupe de révision et de validation.

e) Détermination des frontières fonctionnelles des systèmes composant la liste.

f) Analyse par facteurs de mesure d'importance pour les systèmes qui ont fait l'objet d'une étude de fiabilité. Pour ceux-ci, deux facteurs de mesure d'importance ont été utilisés pour évaluer la criticité de l'équipement soit : Fussel-Vesely (FV) et Risk Achievement Worth (RAW).

g) Consultation avec les responsables techniques de système des systèmes concernés.

h) Révision et validation de ces deux listes par le groupe de révision et de validation.

L'application de cette méthodologie a permis de réviser la liste des SRS de la centrale nucléaire et de déterminer les systèmes considérés comme importants pour la sûreté.

E.2 Les classes de SIS

Les SIS identifiés à la centrale nucléaire ont été regroupés en 6 grandes classes. Puisque la méthodologie développée pour déterminer les objectifs de fiabilité des SIS n'est pas appliquée de la même façon pour certaines de ces classes, il est opportun de les présenter et d'identifier les SIS qui les constituent.

Voici les classes de SIS :

E.2.1 Systèmes spéciaux de sûreté

Système d'arrêt d'urgence #1 (SAU#1) :

Cette famille inclut tous les systèmes et équipements requis pour l'arrêt du réacteur par le SAU#1 lors d'une sollicitation automatique ou manuelle.

Système d'arrêt d'urgence #2 (SAU#2) :

Cette famille inclut tous les systèmes et équipements requis pour l'arrêt du réacteur par le SAU#2 lors d'une sollicitation automatique ou manuelle.

Refroidissement du cœur (RUC) :

Cette famille inclut tous les systèmes et équipements requis pour le refroidissement du combustible par le RUC lors d'une sollicitation automatique ou manuelle.

Confinement :

Cette famille inclut tous les systèmes et équipements requis pour le confinement des matières radioactives ou le contrôle de la surpression dans le bâtiment du réacteur lors d'une sollicitation automatique ou manuelle.

E.2.2 Systèmes de sûreté en attente

Alimentation électrique d'urgence (AEU) :

Cette famille inclut tous les systèmes et équipements requis pour assurer l'alimentation électrique aux charges de l'AEU.

Système d'eau d'urgence (SEU) :

Cette famille inclut tous les systèmes et équipements requis pour assurer l'appoint en eau aux générateurs de vapeur, au caloporteur ou à l'échangeur de chaleur du RUC par le SEU.

E.2.3 Systèmes communs de service

Alimentation électrique de catégorie I (cat. I) :

Cette famille inclut tous les systèmes et équipements requis pour assurer l'alimentation électrique aux charges des barres de la catégorie I par les batteries de cette catégorie électrique.

Alimentation électrique de catégorie II (cat II) :

Cette famille inclut tous les systèmes et équipements requis pour assurer l'alimentation électrique aux charges des barres de la catégorie II par les batteries de cette catégorie.

Alimentation électrique de catégorie III (cat. III) :

Cette famille inclut tous les systèmes et équipements requis pour assurer l'alimentation électrique aux charges essentielles par les générateurs de catégorie III.

Eau de service recirculée (ESR) :

Cette famille inclut tous les systèmes et équipements requis pour assurer le refroidissement des charges essentielles de l'ESR.

Système d'air d'instrumentation (air) :

Cette famille inclut tous les systèmes et équipements requis pour assurer l'alimentation en air aux charges essentielles de l'air d'instrumentation.

E.2.4 Systèmes de procédé

Système du caloporteur :

Cette famille inclut tous les systèmes et équipements qui assurent le refroidissement du combustible dont la défaillance entraîne une perte du refroidissement en raison de température excessive du combustible ou d'une rupture de gaine.

Système de régulation du réacteur (SRR) :

Cette famille inclut certains systèmes et équipements qui assurent le contrôle de la puissance du réacteur dont la défaillance entraîne une perte du refroidissement en raison de température excessive du combustible ou d'une rupture de gaine.

Refroidissement en temps d'arrêt (RTA) :

Cette famille inclut tous les systèmes et équipements qui assurent le refroidissement du combustible en temps d'arrêt dont la défaillance entraîne une perte du refroidissement en raison de température excessive du combustible ou d'une rupture de gaine.

E.2.5 Sources froides de relève

Refroidissement en temps d'arrêt (RTA) :

Cette famille inclut tous les systèmes et équipements dont la défaillance entraîne la perte des RTA comme source froide de relève.

Système du modérateur :

Cette famille inclut tous les systèmes et équipements dont la défaillance entraîne la perte du modérateur comme source froide ultime.

Système auxiliaire d'eau d'alimentation :

Cette famille inclut tous les systèmes et équipements dont la défaillance entraîne la perte de l'alimentation d'eau auxiliaire au secondaire des générateurs de vapeur.

E.2.6 Surveillance

Surveillance :

Cette famille inclut tous les systèmes et équipements qui permettent à l'opérateur de prendre une décision ou une action lors d'un incident. En outre, elle inclut l'habitabilité des salles de commandes principale et d'urgence, les indications permettant à l'opérateur de prendre une décision et la capacité de l'opérateur à prendre action.

E.3 Description des SIS

Une description sommaire des SIS sélectionnés pour la validation de la méthodologie est présentée. Toutefois, il faut préciser que les systèmes de la centrale sont d'une certaine complexité et que les descriptions fournies sont relativement sommaires. Cependant, elles sont suffisantes pour les besoins de ce rapport.

E.3.1 Refroidissement d'urgence du cœur (RUC) :

Le système de refroidissement d'urgence du cœur est un système spécial de sûreté (SSS) qui a été prévu pour maintenir le refroidissement du combustible suite à un accident de perte de caloporteur (PERCA). Il permet l'injection d'eau dans le cœur du

réacteur lors d'une perte de refroidissement caloporteur de façon à assurer le refroidissement immédiat du combustible. De plus, il assure à long terme l'évacuation de la chaleur résiduelle de ce même combustible. Le RUC assure principalement 3 fonctions :

1. Injection d'eau froide
2. Refroidissement ultra-rapide du cœur du réacteur
3. Isolation des boucles du caloporteur

E.3.2 Système d'eau d'urgence (SEU)

Le système d'eau d'urgence est un système de sûreté en attente. Il assure l'évacuation adéquate de la chaleur du réacteur lorsque tous les systèmes de refroidissement sont inopérants (E.S.R., eau alimentation au G.V., R.U.C. et caloporteur) suite à des pannes de catégorie III et IV, des bris de tuyauterie d'eau d'alimentation ou d'un tremblement de terre. Le système remplit sa mission en exécutant les fonctions suivantes :

1. En remplaçant l'eau de service recirculée (E.S.R.) vers l'échangeur de chaleur du RUC.
2. En injectant de l'eau brute aux générateurs de vapeur suite à une panne de catégorie III et IV ou un bris de ligne d'eau d'alimentation ou de vapeur qui se traduit par une baisse de niveau d'eau dans les G.V. du côté secondaire.
3. En injectant de l'eau brute directement dans le système caloporteur suite à une perte du RUC.

E.3.3 Système d'eau de service recirculée (ESR) :

Le système d'eau de service recirculée est une boucle fermée d'eau déminéralisée destinée à refroidir les équipements du B/R, du bâtiment de service (B/S) et du bâtiment turbine (B/T) pour tous les états de la centrale. La principale fonction du système est d'assurer le refroidissement du combustible en temps d'arrêt et des procédés nucléaires

en temps de marche. La boucle est refroidie par l'eau du fleuve (eau brute de refroidissement, EBR) qui passe à travers 4 échangeurs indépendants dont la capacité globale est de quelques 200 MW.

E.3.4 Caloporteur

Le système caloporteur est conçu pour faire circuler de l'eau lourde pressurisée à travers les canaux de combustible du réacteur afin de récupérer la chaleur produite par la fission du combustible d'uranium. La chaleur contenue dans le caloporteur est transférée à de l'eau légère dans les générateurs de vapeur (GV) qui, à leur tour, produisent la vapeur qui entraînera le groupe turboalternateur. Le système est formé de deux circuits fermés qui sont reliés entre eux en plusieurs endroits en marche normale. Le débit à travers le cœur du réacteur est bidirectionnel dans chaque circuit. Les principales composantes du système sont les 380 canaux de combustible du réacteur, les quatre générateurs de vapeur verticaux, les quatre pompes principales, les quatre collecteurs d'entrée, les quatre collecteurs de sortie du réacteur et les deux tuyaux d'équilibrage. Les canaux de combustible sont horizontaux afin d'y avoir accès aux deux bouts avec la machine à chargement de combustible. Les collecteurs, les générateurs de vapeur et les pompes sont situés plus haut que le réacteur afin qu'un thermosiphon s'établisse sur perte des pompes principales.

E.3.5 Modérateur

Le modérateur a pour mission de ralentir les neutrons de haute énergie produits par des fissions afin de favoriser de nouvelles fissions et ainsi maintenir la réaction en chaîne. Il sert aussi de milieu dispersant pour les poisons nucléaires (bore, gadolinium) servant au contrôle de la réactivité dans le cœur du réacteur et maintenir le réacteur à l'arrêt. De plus, le modérateur élimine la chaleur dégagée par le ralentissement des neutrons, l'absorption des rayons gamma provenant de la réaction nucléaire et de celle transmise par conduction en provenance de la calandre et des plaques tubulaires. Finalement, il

sert de réservoir de dispersion de chaleur en cas de perte du caloporteur (PERCA) combinée à une indisponibilité du RUC.

Le système modérateur principal fonctionne à basse pression et à basse température. Il est essentiellement composé de tuyauterie, de 2 pompes centrifuges et de 2 échangeurs de chaleur. L'eau lourde est pompée du bas de la calandre par une des pompes vers les 2 échangeurs de chaleur qui la refroidissent en parallèle, puis elle est retournée vers la calandre par des diffuseurs. En opération normale à pleine puissance, le modérateur dans la calandre s'échauffe à un taux d'environ 95 MW thermique et doit être refroidi et maintenu à une température de 67°C.

ANNEXE F : QUESTIONNAIRE

Ce questionnaire a été établi pour obtenir l'opinion de certains experts de la centrale nucléaire concernant l'établissement des objectifs de fiabilité des SIS. Il a été rédigé dans le but d'éclaircir certains concepts qui permettront de faciliter la détermination des objectifs. En fait, il a été jugé nécessaire de connaître à quoi serviront les objectifs de fiabilité avant de commencer à travailler sur la méthodologie permettant de les déterminer. Le questionnaire se divise en deux parties soit les objectifs de fiabilité et la méthodologie pour les déterminer.

Objectifs de fiabilité :

1- Qu'est-ce qu'un objectif de fiabilité?

2- Pour quelle(s) raison(s) doit-on déterminer des objectifs de fiabilité pour les SIS?

3- Quelles sont les personnes dans une centrale qui sont directement concernées par les objectifs de fiabilité et quels usages en font-elles?

4- À l'heure actuelle, existe-t-il des objectifs de fiabilité pour certains systèmes et comment ont-ils été établis?

5- Comment une centrale s'assure de respecter les objectifs de fiabilité des systèmes, en particulier ceux qui ne possèdent pas d'étude de fiabilité?

6- Quelles seront nos règles d'exploitation dans la LCE si un système ne respecte-pas ses objectifs de fiabilité d'un SIS ?

7- Comment sera calculée la fiabilité d'un SIS sur perte ou retrait volontaire d'un composant redondant et quelles seront nos règles d'exploitation pour la perte d'un composant redondant par rapport aux objectifs de fiabilité des SIS ?

8- Est-ce que les objectifs devraient être révisés de façon périodique pour être représentatifs de nouvelles connaissances, d'un nouvel état de la centrale, etc. ? Si oui, quand un objectif de fiabilité doit-il être révisé ?

9- Les objectifs de fiabilité doivent-ils être établis en s'assurant qu'ils puissent être atteints ou doit-on les fixer sans s'en préoccuper et des mesures seront prises ensuite pour les respecter?

10- Est-ce que les objectifs de fiabilité doivent être fixés strictement en fonction de la protection du public, strictement de la pérennité des exploitations (préoccupations économiques), des deux ou encore y-a-t-il d'autres facteurs à considérer?

Méthodologie :

1- Est-ce que les valeurs créditées dans les ÉMS présentent une valeur du risque jugé acceptable ?

Si oui ,

a. Que faire avec les systèmes qui ne sont pas crédités dans les matrices pour déterminer le risque acceptable?
b. Est-ce qu'il faut prendre la probabilité créditée de défaillance du système dans l'ÉMS ou la probabilité créditée de défaillance multipliée par la probabilité que le système soit sollicité (séquence d'événements)?

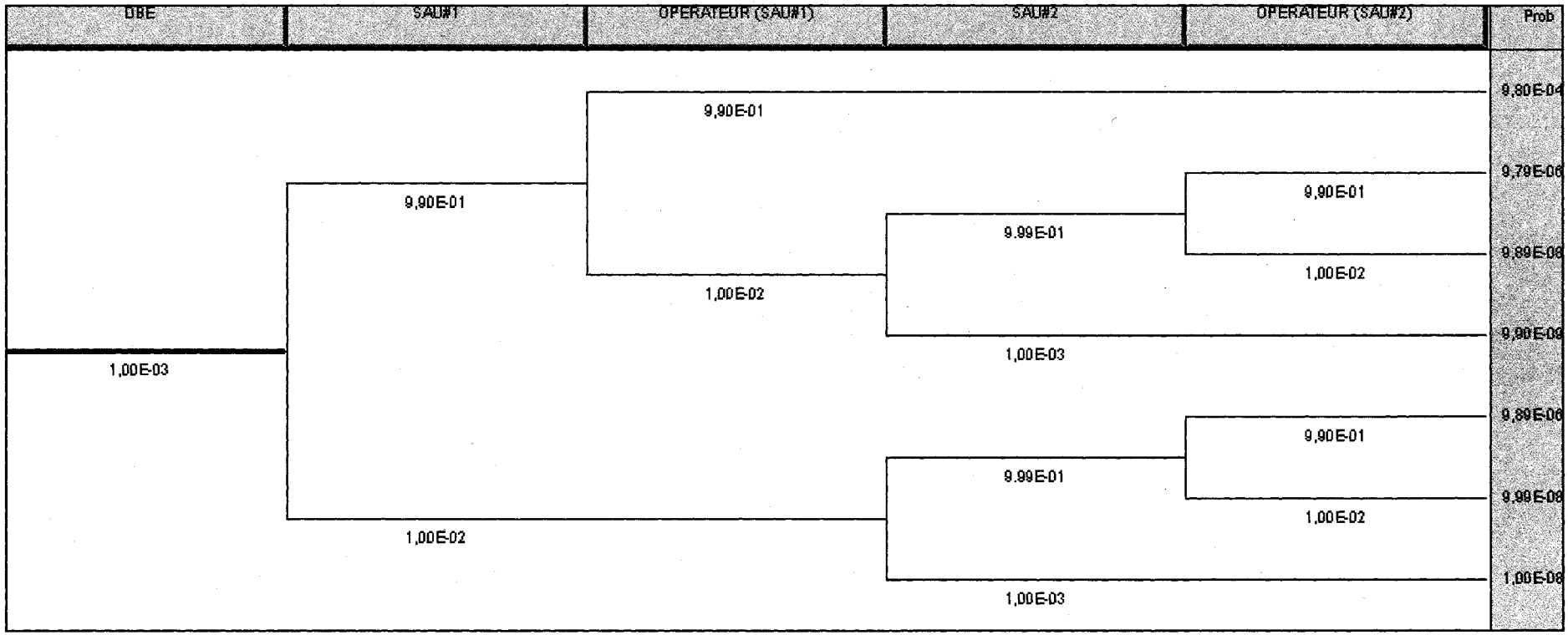
2- Que faire avec les SIS qui n'ont pas d'étude de fiabilité pour s'assurer qu'ils répondent aux objectifs de fiabilité?

3- Quels sont les facteurs importants à considérer pour juger l'importance des conséquences de la défaillance d'un SIS?

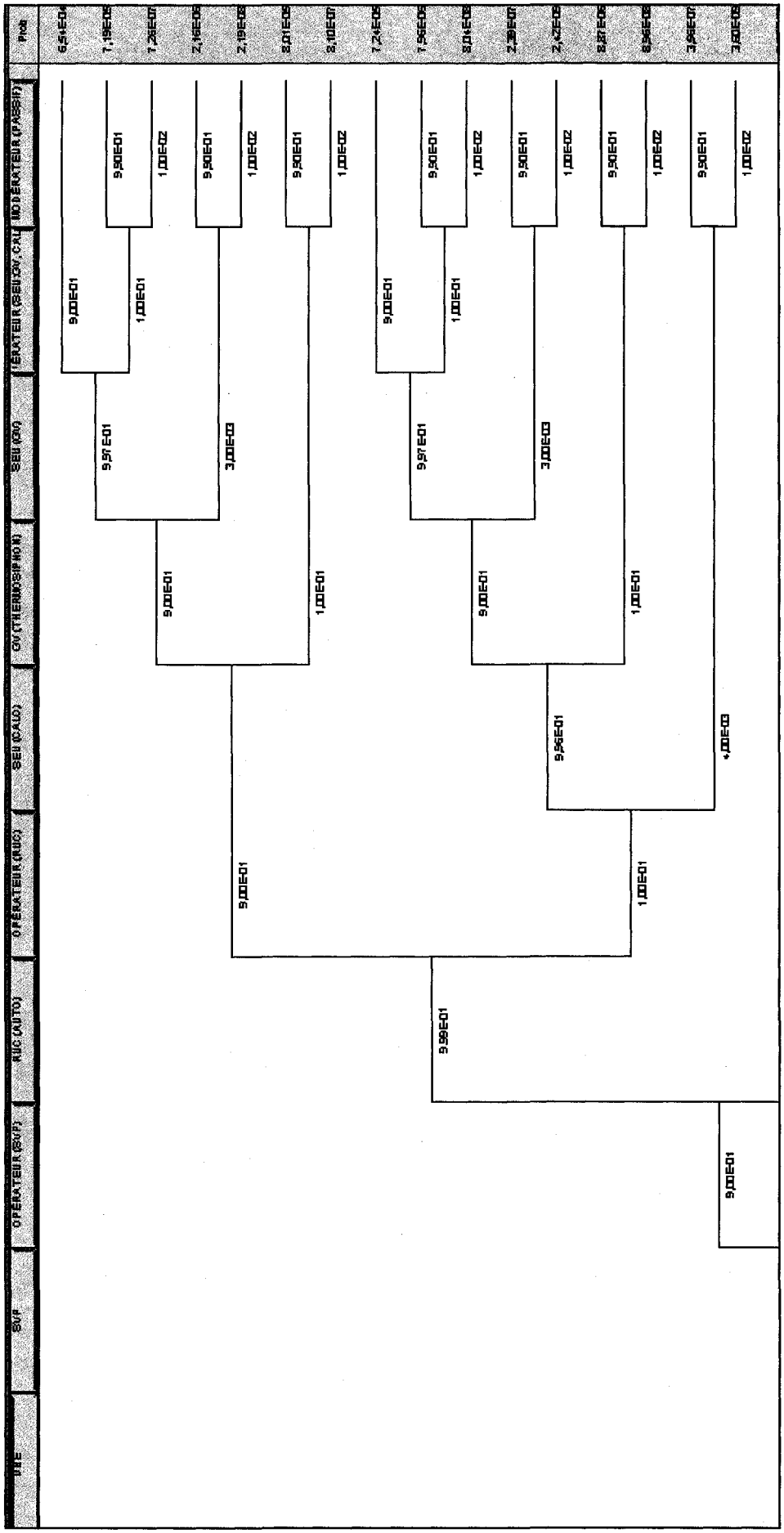
ANNEXE G : SÉQUENCES D'ÉVÉNEMENTS

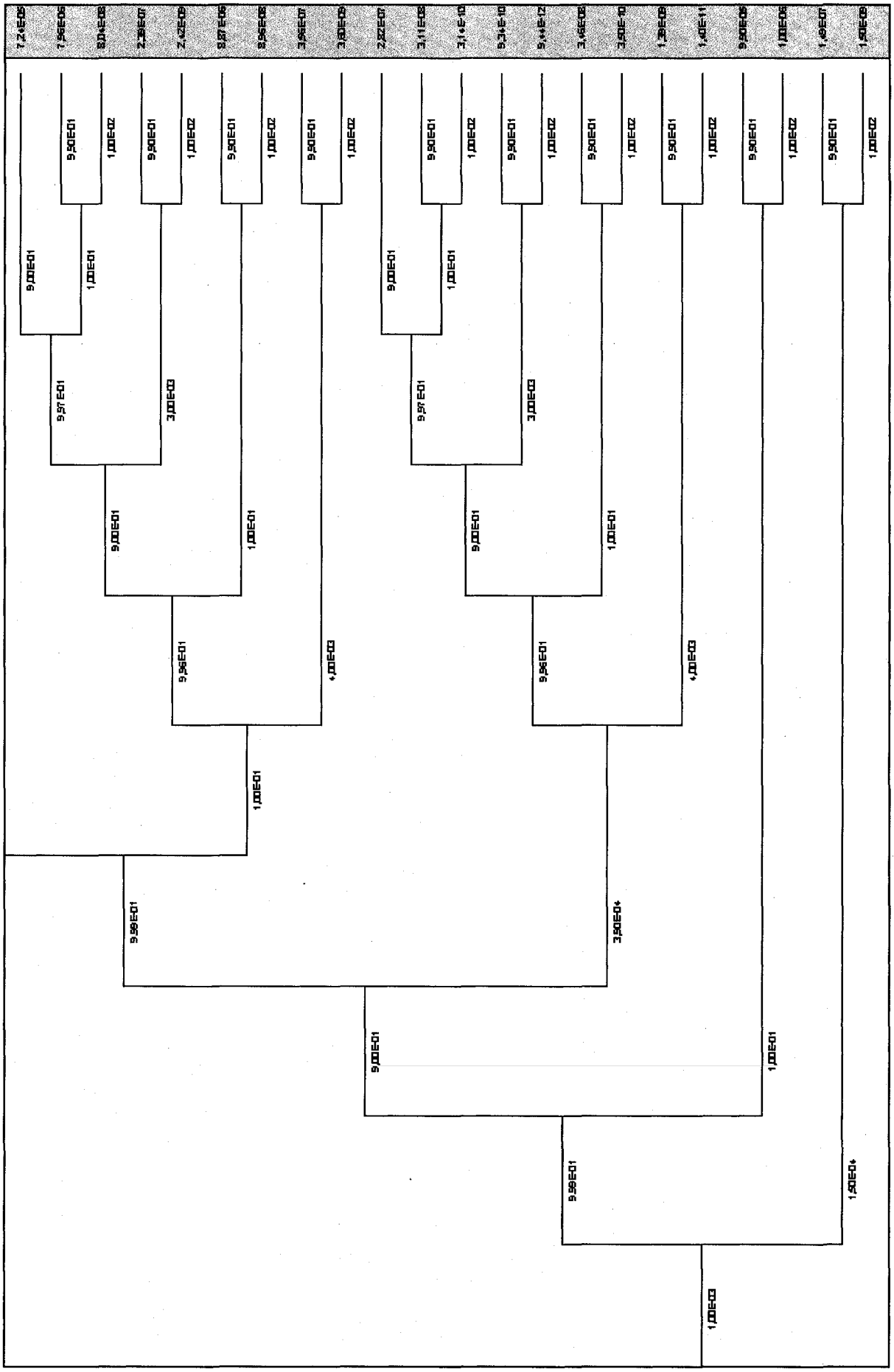
Les séquences d'événement ont été développées de façon à être représentatives de la gestion d'incident à la centrale nucléaire. Elles ont été élaborées de concert à l'ingénieur responsable des procédures d'exploitation sur incident (PEI). Voici les séquences développées dans le cadre de ces travaux.

DBE (arrêt du réacteur)

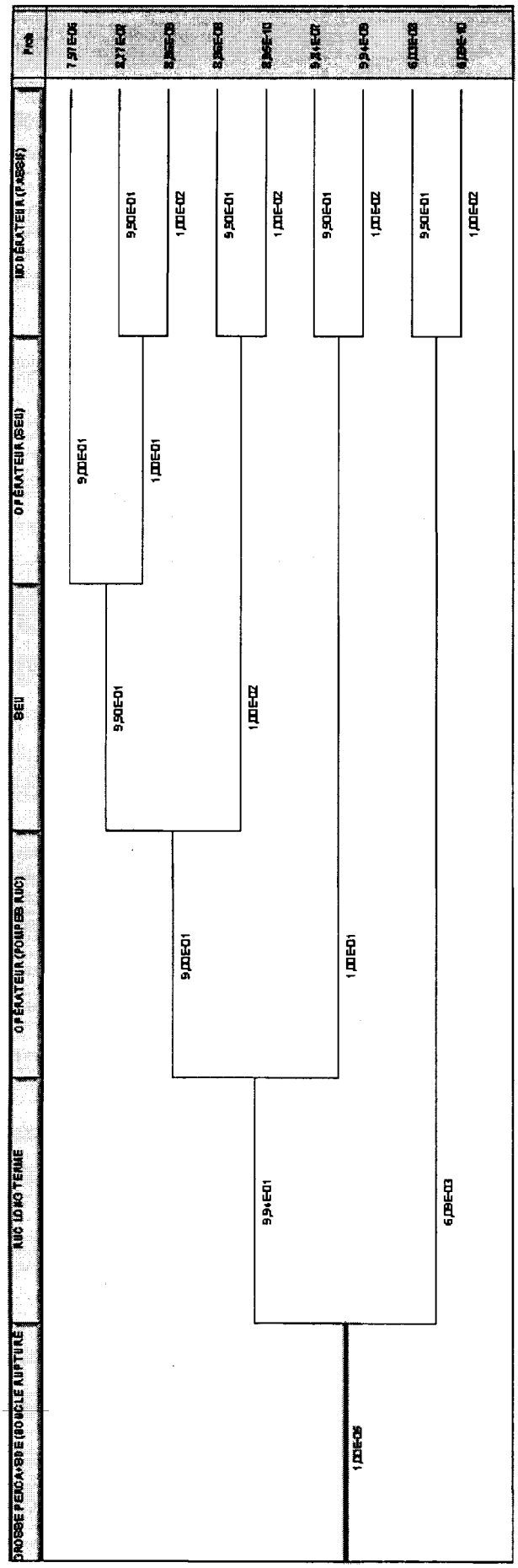


DBE :

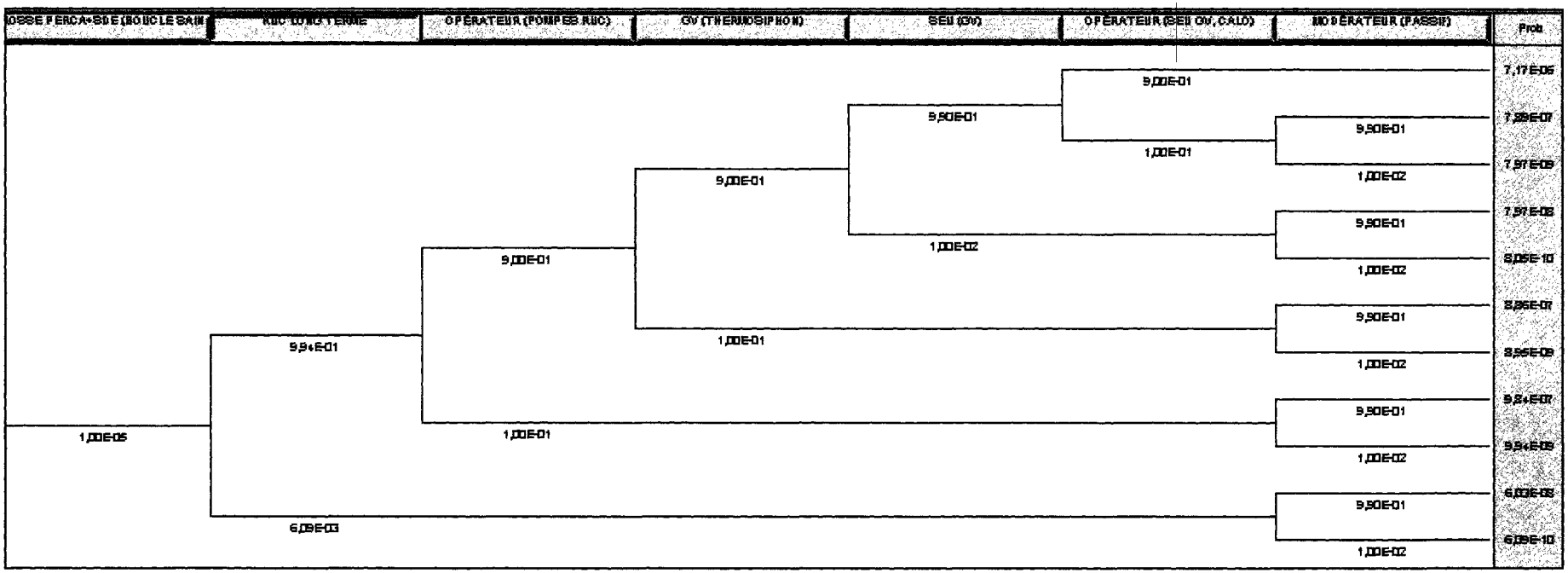

Prob
IDDEFAILLEMASSIF
TENATEUR(SEUIL2W,CX
SEUIL(2W)
OVTHENUSSIHOM
SEUIL(CALC)
OPERATEUR(AUC)
AUC(AUTO)
OPERATEUR(SUP)
SUP
DBE



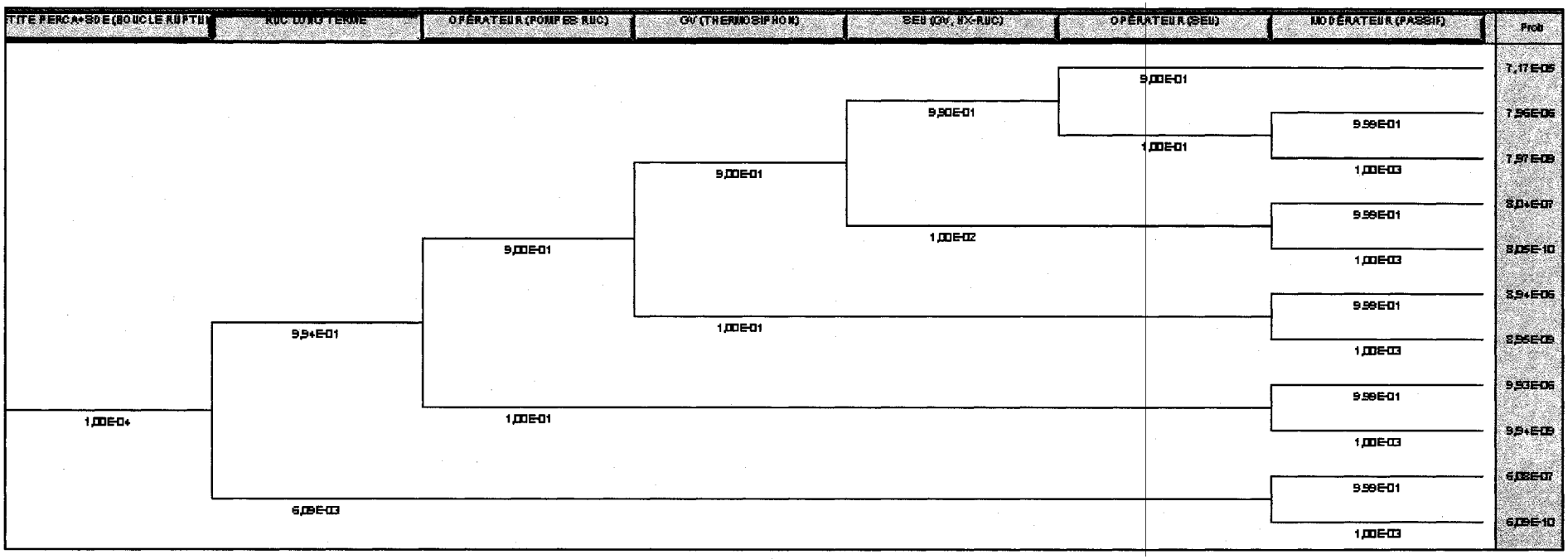
Grosse PERCA + SDE 24 heures après (boucle rupturée)



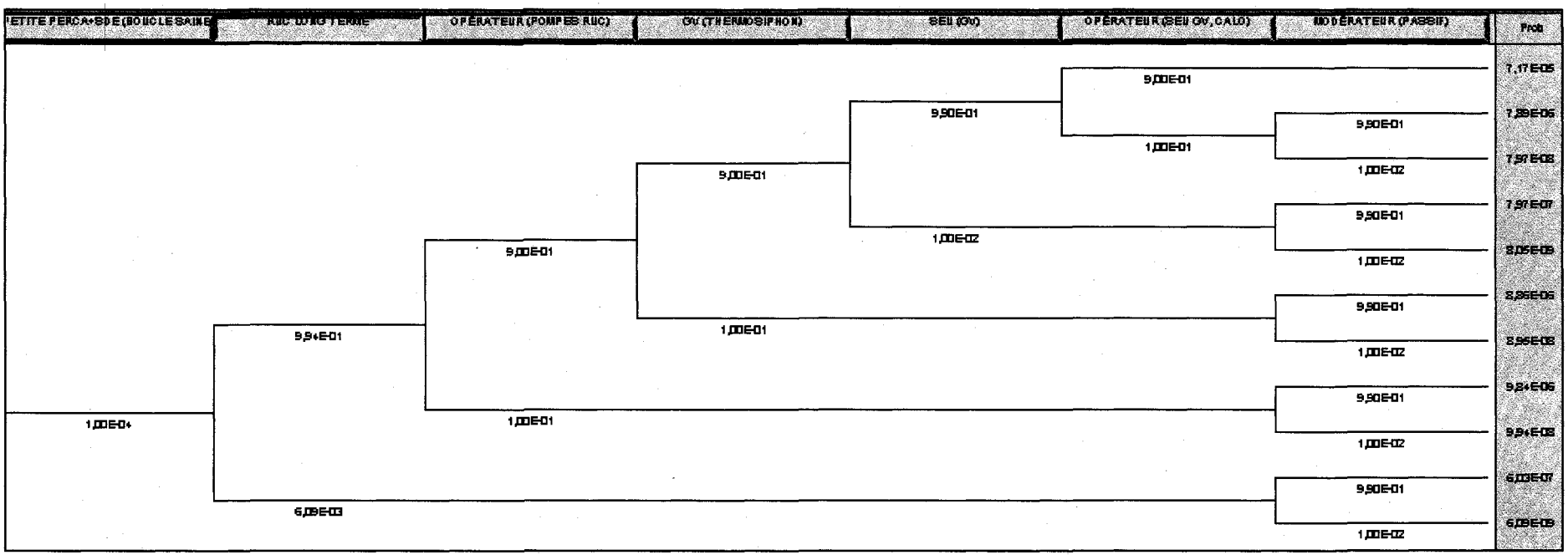
Grosse PERCA + SDE 24 heures après (boucle saine)



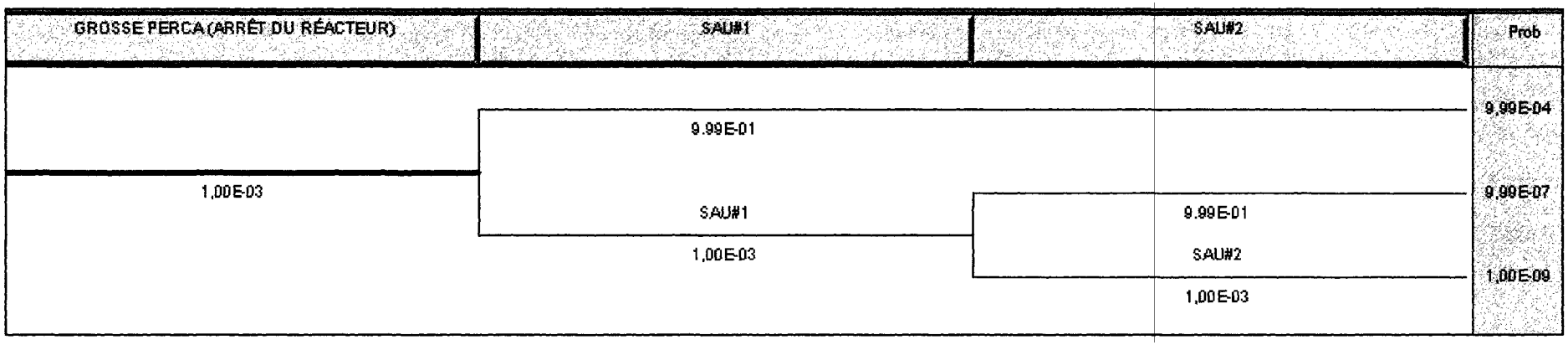
Petite PERCA + SDE 24 heures après (boucle rupturée)



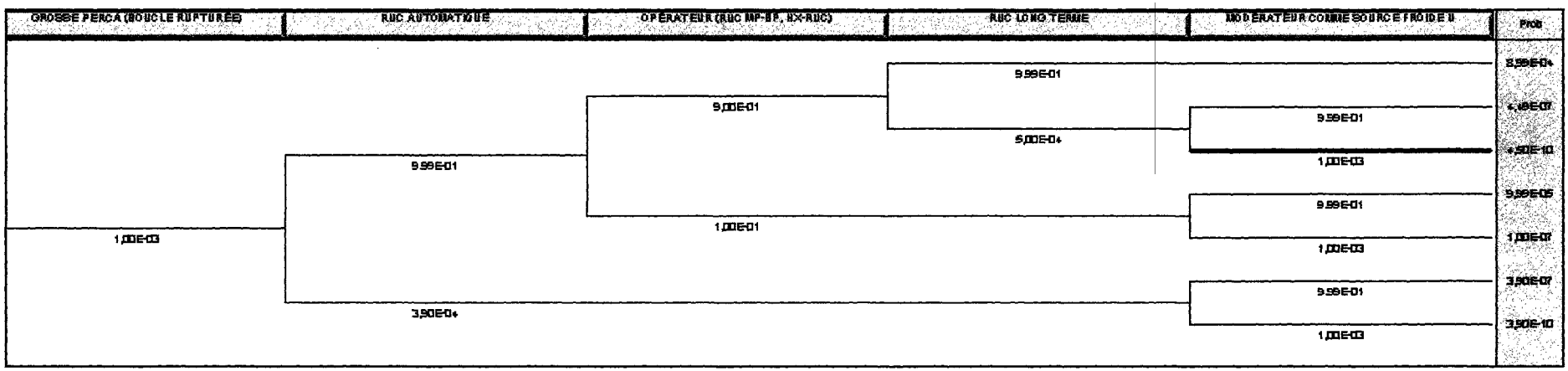
Petite PERCA + SDE 24 heures après (boucle saine)



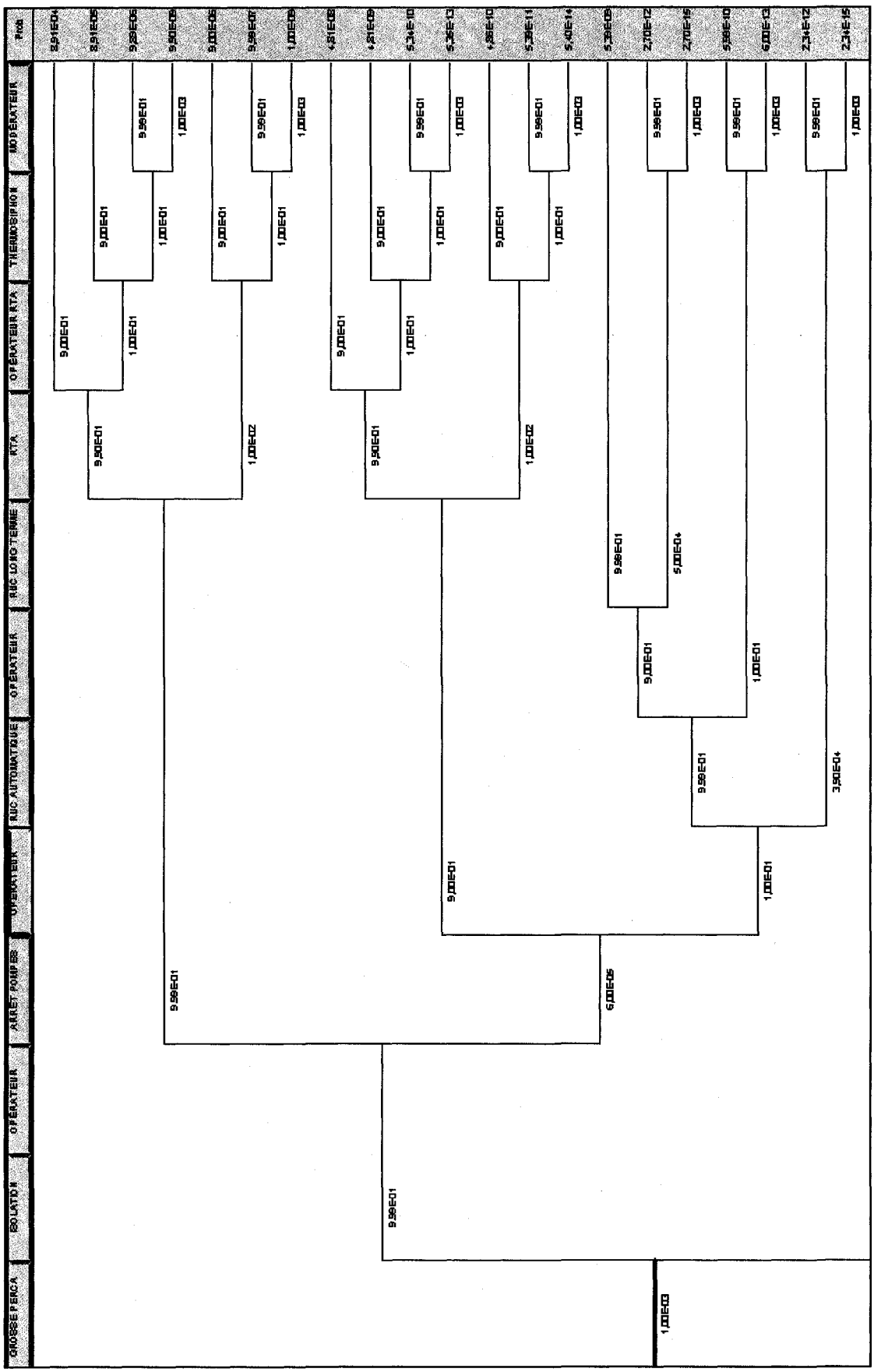
Grosse PERCA (arrêt du réacteur)

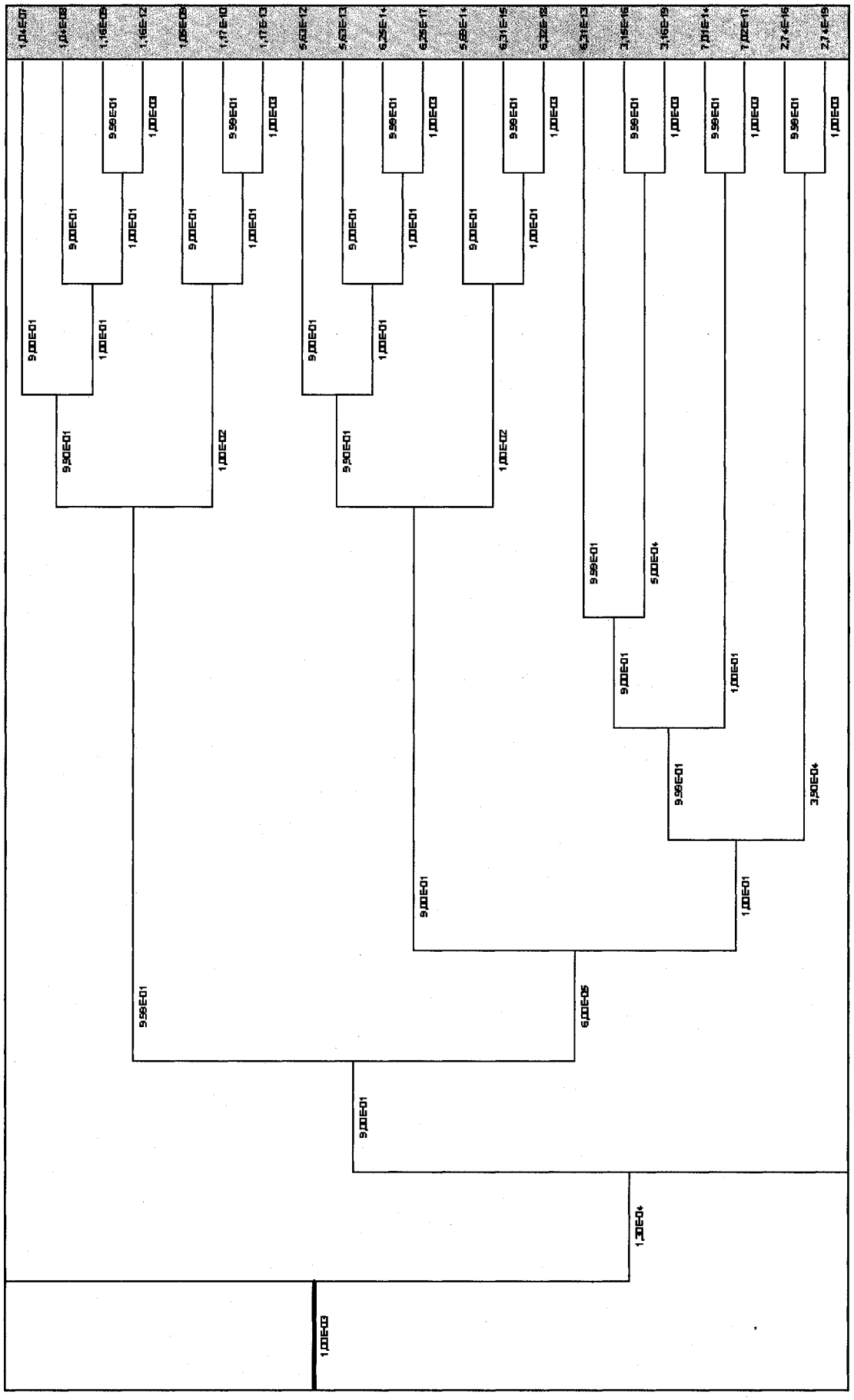


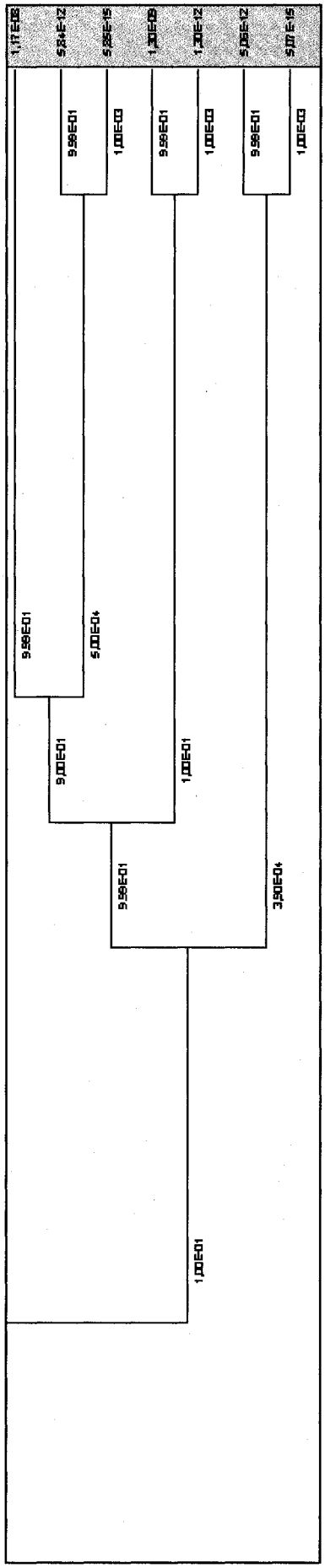
Grosse PERCA (boucle rupturée)



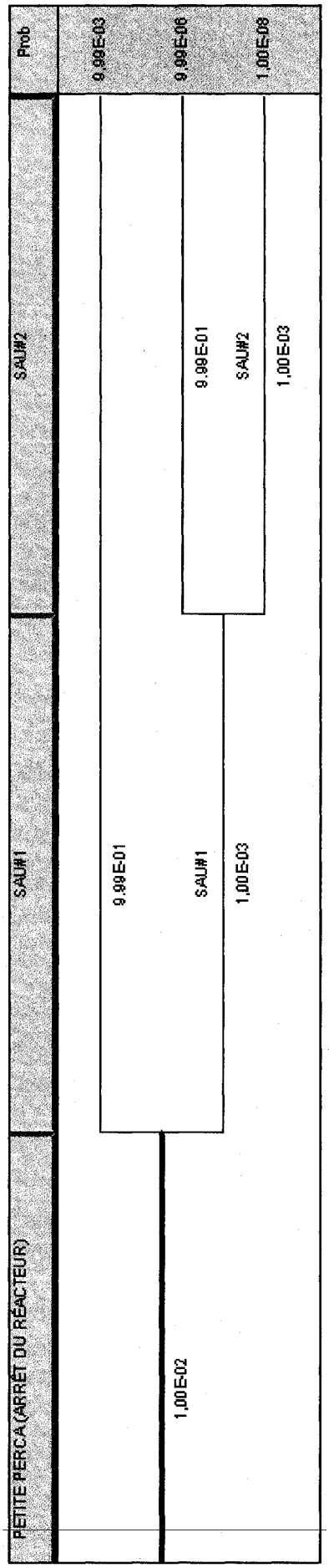
Grosse PERCA (boucle saine)



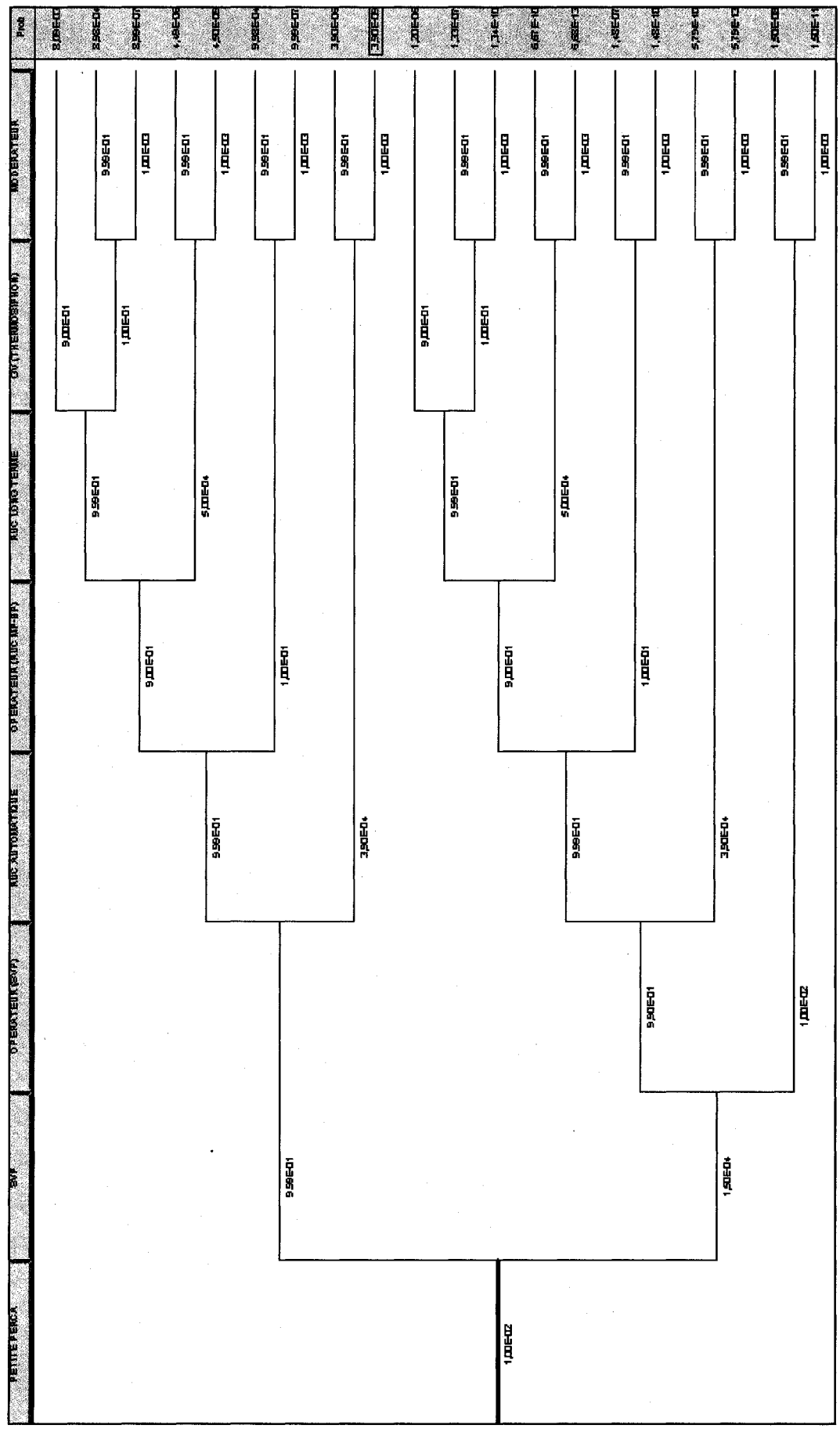




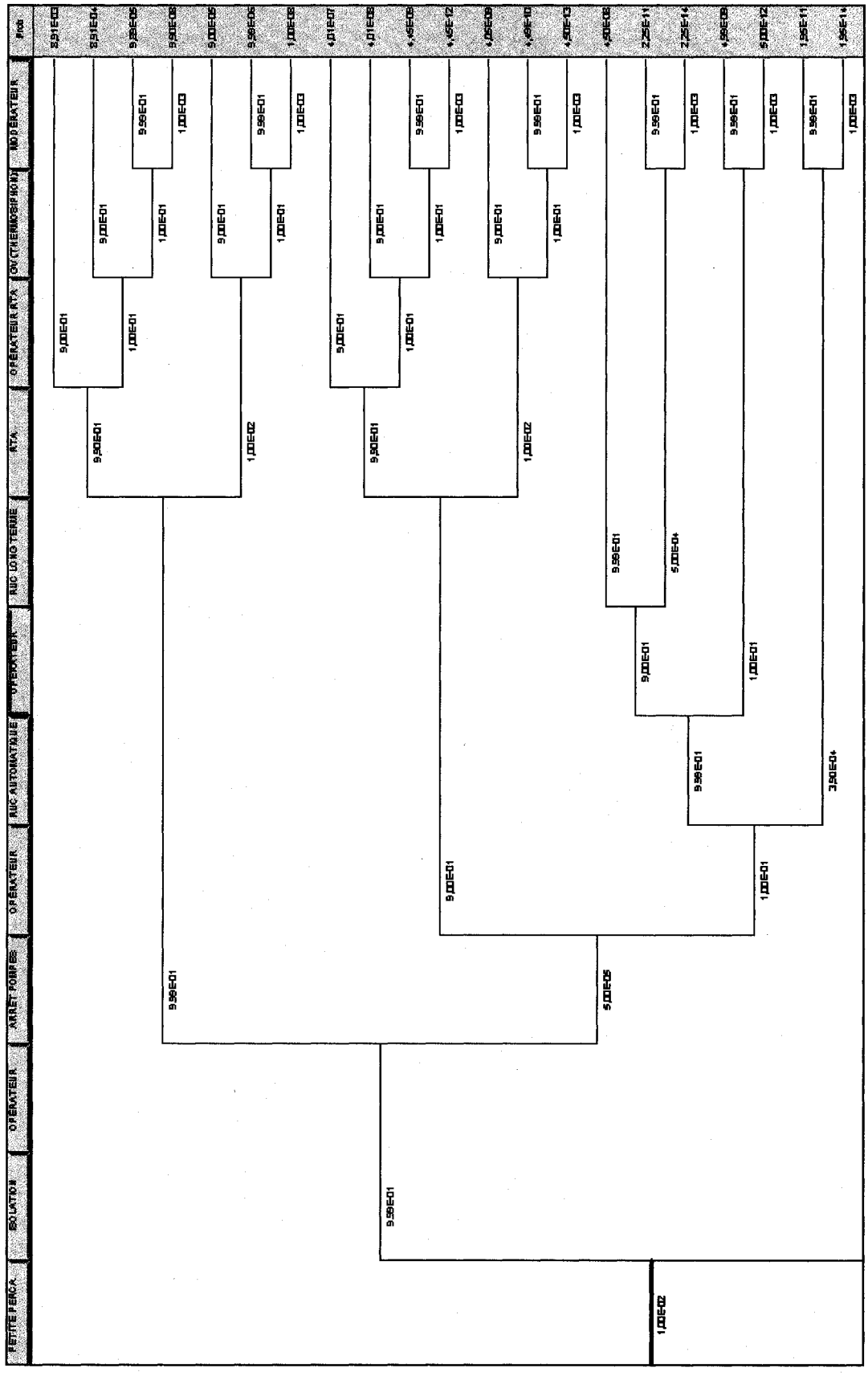
Petite PERCA (arrêt du réacteur)

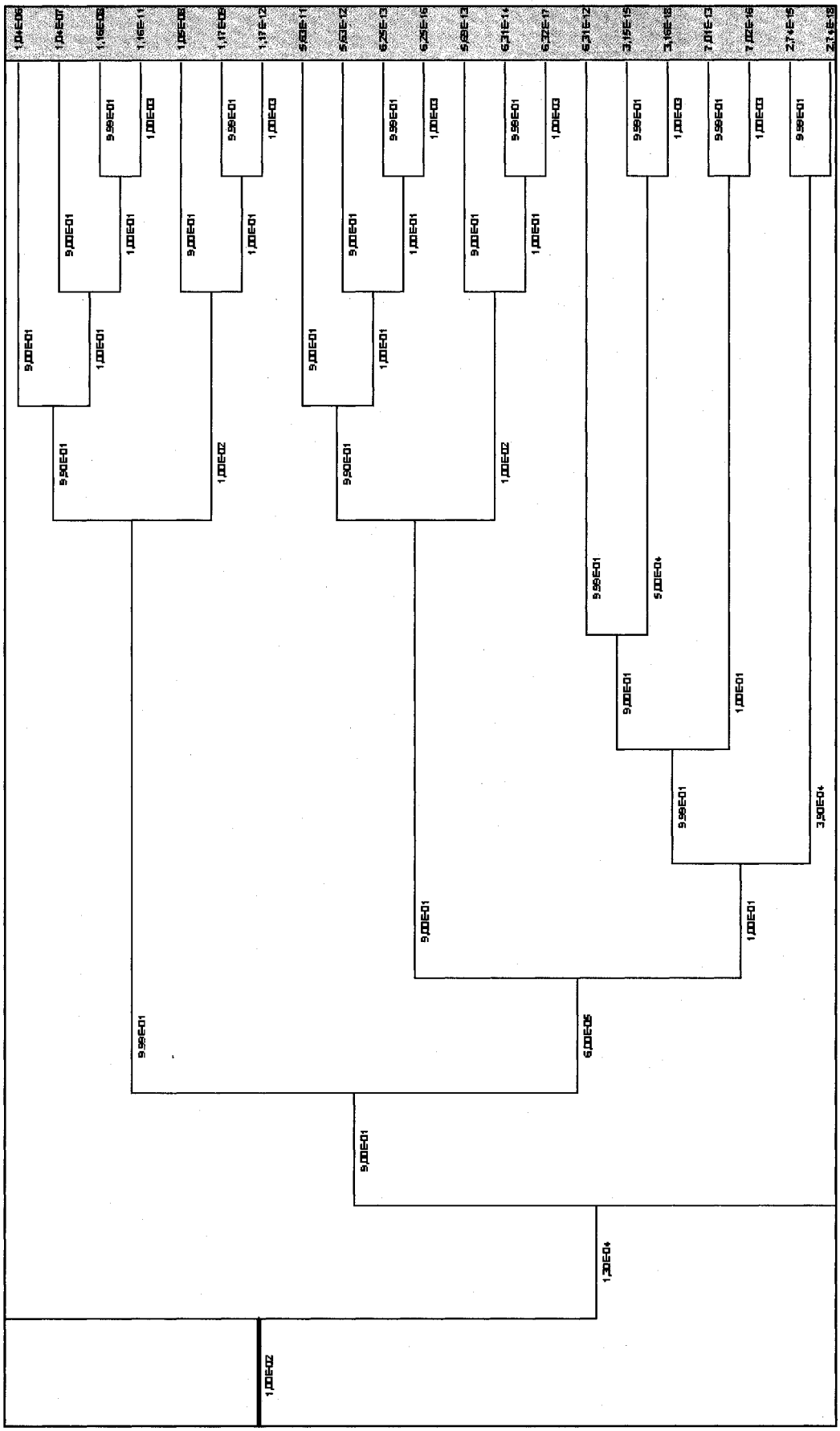


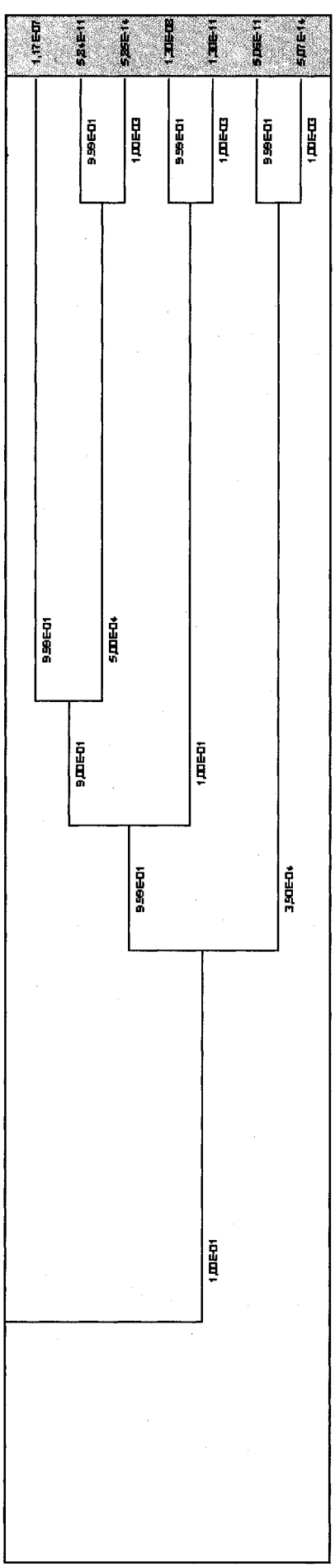
Petite PERCA (boucle rupturée)



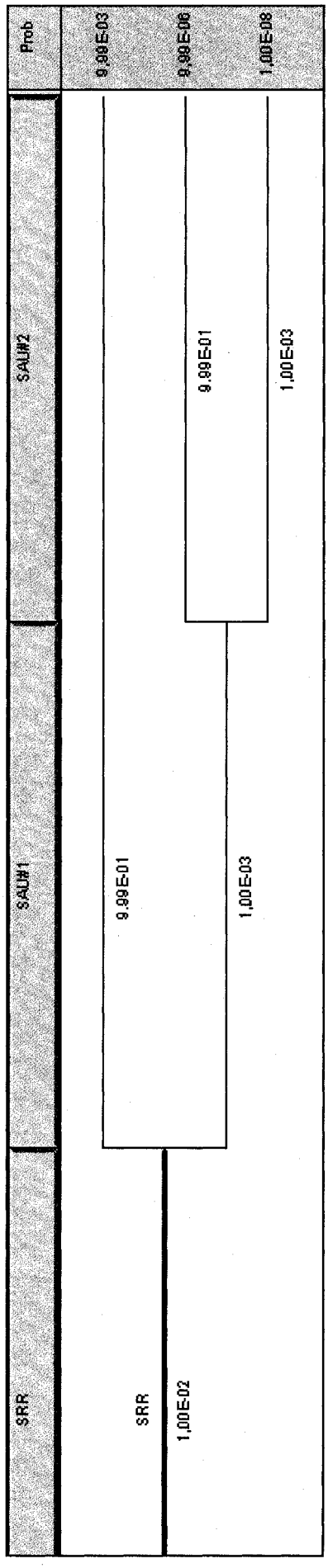
Petite PERCA (boucle saine)




1.04E-06
1.04E-07
1.16E-10
1.16E-11
1.15E-08
1.17E-08
1.17E-12
5.63E-11
5.63E-12
6.25E-13
6.25E-16
5.62E-13
6.31E-14
6.32E-17
6.31E-12
3.15E-15
3.16E-18
7.01E-13
7.02E-16
2.7E-15
2.1E-13
9.99E-01
1.00E-03
9.00E-01
1.00E-01
9.50E-01
1.00E-02
9.90E-01
5.00E-04
6.00E-05
1.20E-04
3.50E-04
1.00E-02

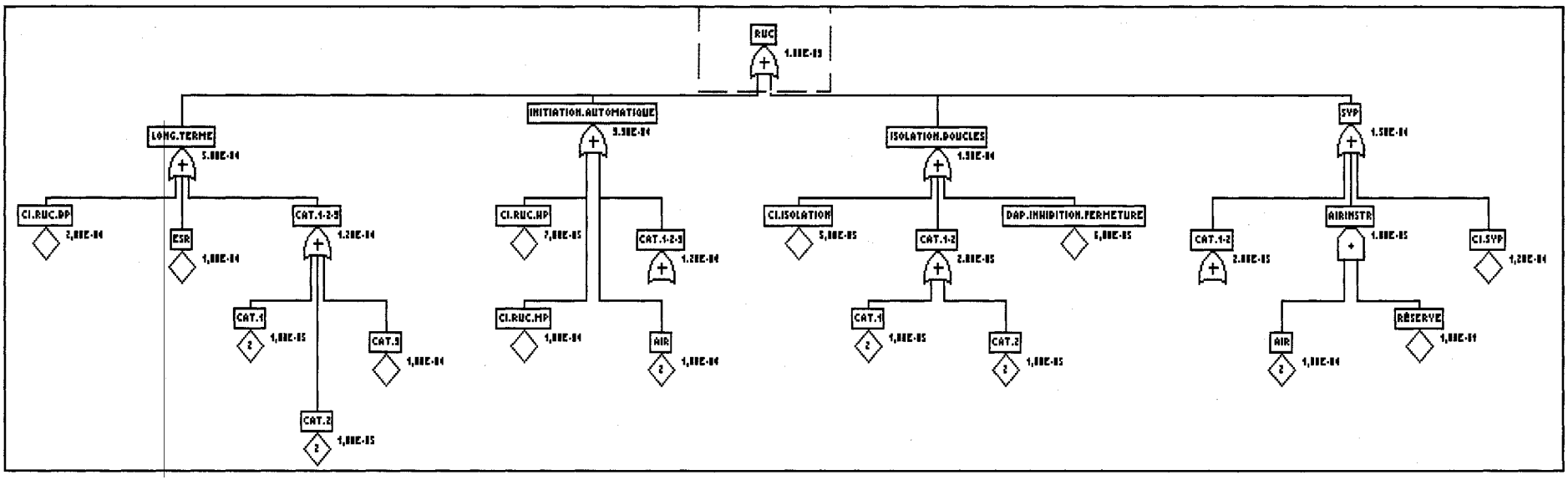

1.17E-07
5.24E-11
5.25E-14
1.31E-08
1.33E-11
5.05E-11
5.07E-14
9.98E-01
1.00E-03
9.99E-01
1.00E-03
9.99E-01
1.00E-03
9.98E-01
1.00E-03
9.98E-01
5.00E-04
9.00E-01
1.00E-01
9.99E-01
3.50E-04
1.00E-01

SRR

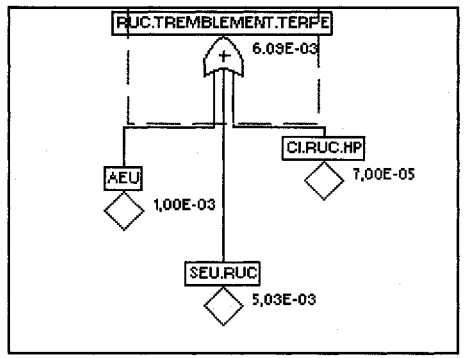

Prob
SAU#2
SAU#1
SRR
9.99E-03
9.99E-06
1.00E-08
9.99E-01
1.00E-03
9.99E-01
1.00E-03
SRR
1.00E-02

ANNEXE H : ARBRES DE DÉFAILLANCE SIMPLIFIÉS

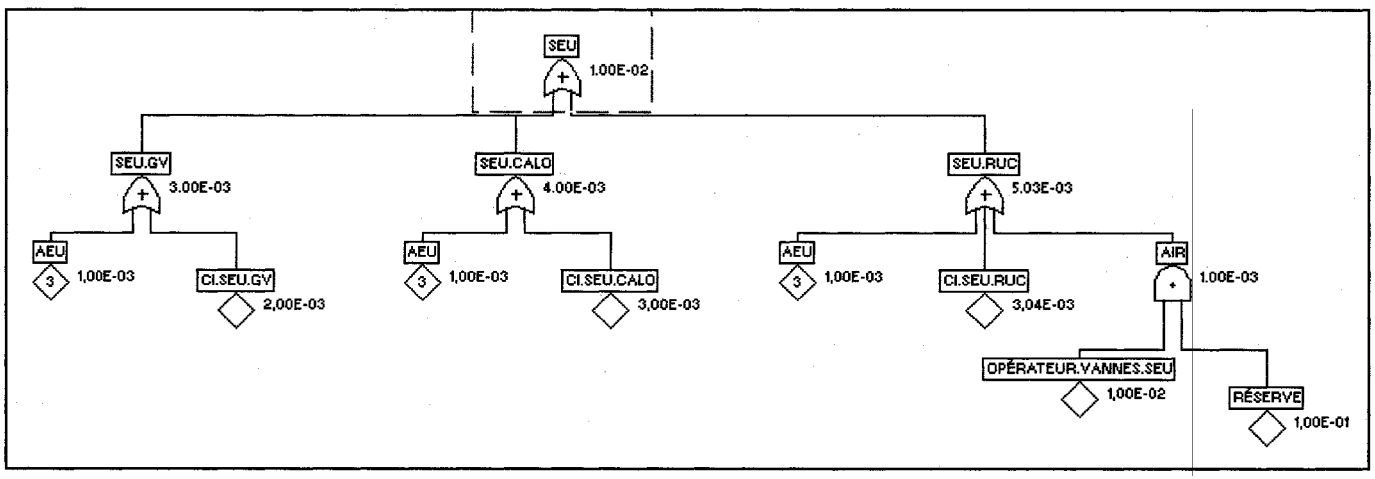
RUC



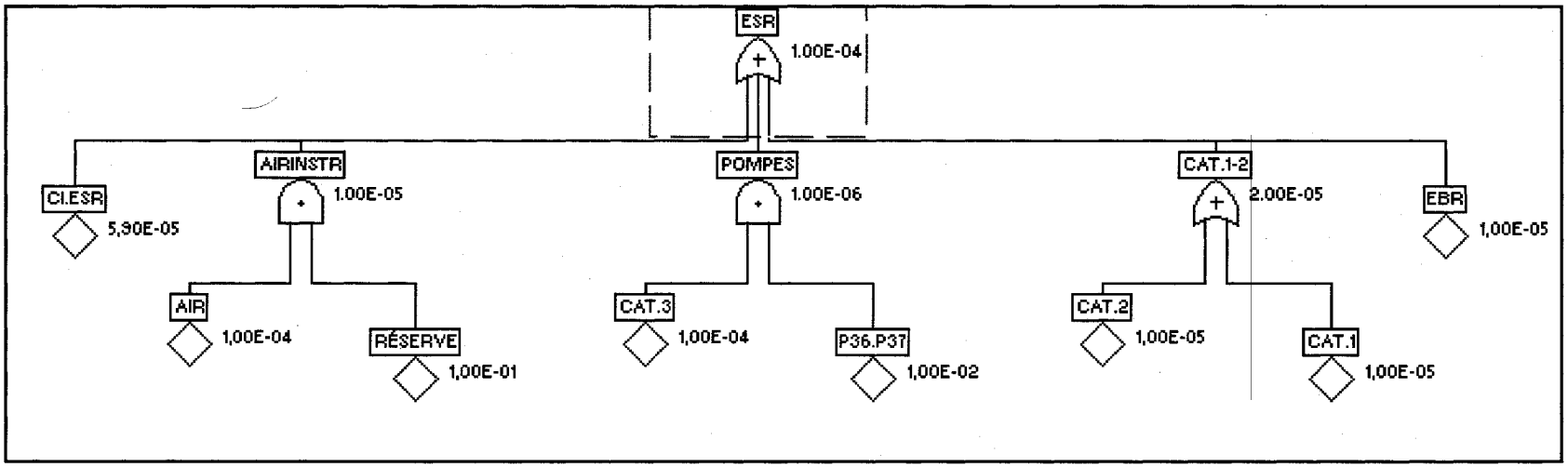
RUC (tremblement de terre)



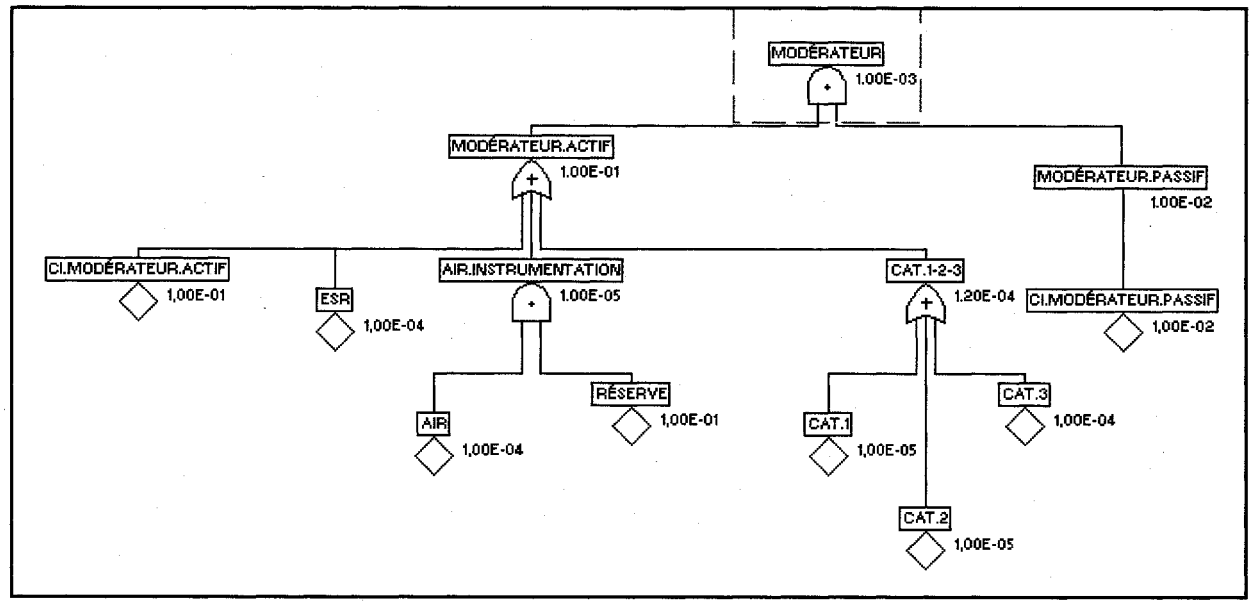
SEU



ESR


ESR
1.00E-04
CI.ESR
5,90E-05
AIRINSTR
1.00E-05
AIR
1,00E-04
RÉSERVE
1,00E-01
POMPES
1.00E-06
CAT.3
1,00E-04
P36.P37
1,00E-02
CAT.1-2
2.00E-05
CAT.2
1,00E-05
CAT.1
1,00E-05
EBR
1,00E-05

Modérateur


MODÉRATEUR
1.00E-03
MODÉRATEUR.ACTIF
1.00E-01
MODÉRATEUR.PASSIF
1.00E-02
CI.MODÉRATEUR.ACTIF
1,00E-01
ESR
1,00E-04
AIR.INSTRUMENTATION
1.00E-05
CAT.1-2-3
1.20E-04
CI.MODÉRATEUR.PASSIF
1,00E-02
AIR
1,00E-04
RÉSERVE
1,00E-01
CAT.1
1,00E-05
CAT.3
1,00E-04
CAT.2
1,00E-05

ANNEXE I : AMDEC DES SIS

Système	Fonction de sûreté	Sous-Fonction de sûreté	État de centrale	Mode de défaillance	Sévérité	PÉC	VP	Criticité
RUC	- Confinement - Refroidissement du combustible	▪ Intégrité du B/R ▪ Maintien de l'inventaire primaire ▪ Refroidissement du fluide caloporteur ▪ Circulation dans tous les canaux de combustible ▪ Contrôle de la pression caloporteur ▪ Évacuation de la chaleur produite dans le caloporteur ▪ Maintien de l'inventaire des GV	A	1 à 10	270	8,30E-01	1,00E-03	Élevé
			B	7, 8, 9 et 10	205	1,70E-01	1,00E-02	Élevé
			C	1 à 10	370	1,00E-04	1,00E-02	Moyen

États de centrale :

A. Centrale en puissance;
B. Centrale à l'arrêt planifié ;
C. PERCA suivi d'un SDE 24 heures après.

Modes de défaillance :

1. Incapacité à détecter une situation requérant l'initiation automatique RUC.
2. Incapacité à détecter une situation requérant l'isolation automatique des boucles du caloporteur.
3. Incapacité à procéder à l'isolation de la boucle intacte lorsque requis
4. Incapacité à assurer le refroidissement ultra-rapide des GV
5. Incapacité à fournir le débit requis pour le fonctionnement efficace du RUC-HP
6. Incapacité à isoler le RUC-HP après son injection
7. Incapacité à fournir le débit requis pour le fonctionnement efficace du RUC-MP
8. Incapacité de réaliser le passage manuel du RUC-MP vers le RUC-BP
9. Incapacité à fournir le débit requis pour le fonctionnement efficace du RUC-BP
10. Incapacité à fournir le débit requis au secondaire de l'échangeur du RUC.

Système	Fonction de sûreté	Sous-Fonction de sûreté	État de centrale	Mode de défaillance	Sévérité	PÉF	VP	Criticité
SEU	- Confinement des produits radioactifs - Refroidissement du combustible	▪ Étanchéité du B/R ▪ Maintien de l'inventaire primaire ▪ Maintien de l'inventaire des GV ▪ Évacuation de la chaleur produite dans le caloporteur	A	1 à 4	105	8,30E-01	1,00E-02	Bas
			B	1 à 4	105	1,70E-01	1,00E-02	Bas
			C	1 à 4	330	1,00E-04	1,00E-02	Moyen

États de centrale :

A. Exploitation en puissance;
B. Centrale à l'arrêt planifié ;
C. PERCA suivi d'un SDE 24 heures après

Modes de défaillance :

1. Perte de l'alimentation d'eau d'urgence au caloporteur ;
2. Perte de l'alimentation d'eau d'urgence aux GV ;
3. Perte de l'alimentation d'eau d'urgence au secondaire de l'échangeur du RUC ;
4. Perte de l'alimentation d'eau d'urgence simultanée au secondaire de l'échangeur du RUC et aux GV

Système	Fonction de sûreté	Sous-Fonction de sûreté	État de centrale	Mode de défaillance	Sévérité	PÉC	VP	Criticité
ESR	- Refroidissement du combustible	▪ Évacuation de la chaleur produite dans le caloporteur	1	1 à 4	200	8,30E-01	1,00E-04	Moyen
			2	1 à 4	220	1,70E-01	1,00E-04	Moyen
			3	1 à 4	195	1,00E-01	1,00E-04	Moyen

États de centrale :

A. Exploitation en puissance;
B. Centrale à l'arrêt planifié ;
C. Situation d'urgence (Perte de catégorie 4, etc.)

Modes de défaillance :

1. Incapacité à assurer le refroidissement des charges de l'ESR
2. Incapacité de procéder à la relâche de charges lors d'une perte de catégorie IV
3. Incapacité de démarrer les pompes de relève ESR lors d'une perte de catégorie IV
4. Incapacité d'assurer un refroidissement de relève aux systèmes essentiels suite à une perte d'ESR

Système	Fonction de sûreté	Sous-Fonction de sûreté	État de centrale	Mode de défaillance	Sévérité	PÉC	PV	Criticité
Grosse PERCA	- Confinement des produits radioactifs - Refroidissement du combustible	▪ Étanchéité du B/R ▪ Maintien de l'inventaire primaire ▪ Circulation dans tous les canaux de combustible ▪ Maintien de l'intégrité de l'enveloppe du caloporteur ▪ Évacuation de la chaleur produite dans le caloporteur ▪ Maintien de l'inventaire des GV ▪ Refroidissement du fluide caloporteur	A	1 à 4	230	8,30E-01	1,00E-03	Élevé
			B	1 à 4	185	1,70E-01	1,00E-03	Moyen
			C	1 à 4	290	1,00E-01	1,00E-03	Moyen

États de centrale :

A. Exploitation en puissance ;
B. Centrale à l'arrêt planifié ;
C. Situation d'urgence.

Modes de défaillance :

1- Incapacité d'assurer le refroidissement adéquat du combustible (centrale à 100% P.P.)
2- Incapacité d'assurer le refroidissement adéquat du combustible (réacteur à l'arrêt, caloporteur chaud et pressurisé) avec les GV comme source froide
3- Incapacité d'alimenter les GV suite à une perte de catégorie IV
4- Incapacité d'assurer le refroidissement du système caloporteur par dépressurisation des GV

Système	Fonction de sûreté	Sous-Fonction de sûreté	État de centrale	Mode de défaillance	Sévérité	PÉC	VP	Criticité
Modérateur	- Confinement - Arrêt du réacteur - Refroidissement	▪ Étanchéité du B/R ▪ Maintien de l'intégrité de l'enveloppe du modérateur ▪ Maintien de la sous-criticité ▪ Évacuation de la chaleur produite dans le caloporteur	A	1 et 3	325	8,30E-01	1,00E-03	Élevé
			B	1 et 3	365	1,70E-01	1,00E-04	Élevé
			C	1 à 3	405	1,00E-01	1,00E-03	Élevé

États de centrale

A. Exploitation en puissance
B. Centrale à l'arrêt planifié ;
C. Situation d'urgence (PERCA, perte de l'alimentation électrique de catégorie III et IV, etc.)

Modes de défaillance

1. Incapacité d'évacuer la chaleur normalement transmise par le combustible au modérateur.
2. Incapacité à assurer le refroidissement du combustible comme source froide ultime dans le cas d'une PERCA combinée à une indisponibilité du RUC.
3. Incapacité à assurer un milieu adéquat à l'efficacité du SAU#2 et au maintien de la sous-criticité par poisons.